Manual de Usuario V 2.0

Contenido

Antes de Comenzar

Lo que debe saber

Aviso: No trate de darle servicio al dispositivo usted mismo, excepto como se explica en su documentación en línea o con otras instrucciones. Siempre siga esta guía de usuario.

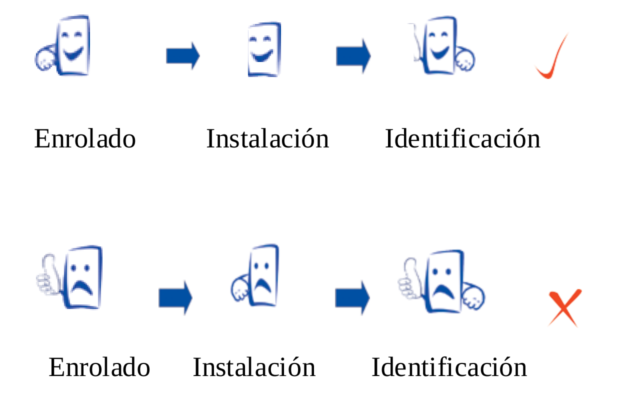
● Por favor no coloque el producto en un lugar con mucha luz, porque la luz excesiva puede afectar considerablemente el escaneo de huellas, y así causar una verificación de huella errónea. Este producto esta diseñado para interiores, si es instalado en exteriores por favor coloque el equipo en un ambiente apropiado, debe tener cuidado de no exponerlo a condiciones húmedas o extremas, el rango de temperatura a la que trabaja el equipo es 0-40℃. No utilice el equipo en lugares muy calientes, manténgalo alejado del fuego. El uso por largo periodo de tiempo en el exterior y el calor interno pueden causar mal funcionamiento del equipo.

●El equipo lector de huellas es un equipo de precisión electrónica, todas las instrucciones de operación y seguridad deben ser leídas antes de comenzar a usar el producto.

● La garantía del producto no cubre daños o defectos ocasionados por defectos de bloqueo, instalación inapropiada, falta de o mal mantenimiento, mal almacenamiento, manejo y transportación,

desgaste ordinario, mal uso, accidente de servicio no autorizado o uso con partes no autorizadas.

Enrolado e Identificación de huellas se tomara después de la instalación del equipo



Como poner la huella

Asegúrese de que la imagen de la huella es el centro del dedo puesto, si coloco bien el dedo y el dispositivo capturó el centro de la huella no tendrá problemas.

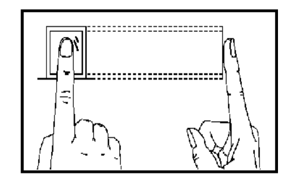
Para tener mayor éxito enrole el mismo dedo 3 veces en un ángulo ligeramente ajustado, uno en el centro, uno inclinado un poco hacia la izquierda y el tercero inclinado un poco hacia la derecha. Si sigue estos procedimientos con seguridad tendrá un enrolado

exitoso.

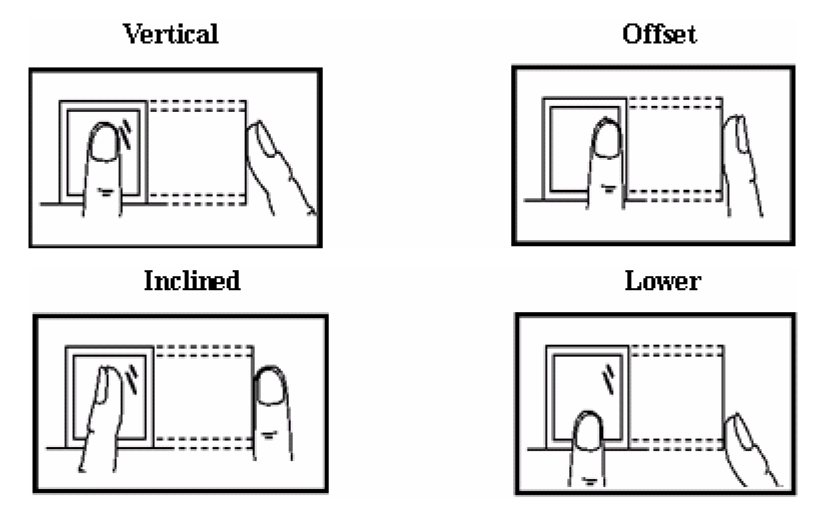
La forma correcta es:

Coloque un dedo cubriendo la superficie del sensor

Colóquelo en el centro de la superficie del sensor



La forma incorrecta es:



Aviso: Por favor adopte la forma correcta para colocar el dedo; La empresa no se hace responsable por daños o problema alguno derivado por el mal uso.

Entendiendo los LEDs del panel de operaciones

Hay diferentes significados para los LEDs del panel de operaciones dependiendo de sus secuencias. Los LEDs que están apagados, encendidos o parpadeando indican el trabajo del lector de huellas.

1. Trabajo normal.
   Luz verde parpadea cada segundo.
2. Autenticación fallida
   Luz roja enciende durante 3 segundos
3. Verificación exitosa
   Luz verde enciende durante 3 segundos

Aviso: Si los LEDs del lector de huellas no corresponden a la descripción anterior por favor contáctenos para darle asistencia técnica.

2

Árbol de Menú

★Indica que este elemento del menú solo aparece en determinados lectores de huellas, este manual dará una instrucción especial.

Conceptos básicos

Esta sección contiene definiciones y descripciones del sistema lector de huellas, incluyendo:

- Enrolado de usuarios
- Verificación de usuarios
- Coincidencia de niveles de umbral
- Números ID de usuario
- Niveles (Estado) de privilegios

Las dos funciones más importantes del lector de huellas son enrolado de usuarios y verificación de usuarios.

Enrolado de usuarios

El enrolado es el procedimiento para crear el numero de ID y escanear un dedo de usuario tres veces para crear una plantilla. Esta plantilla está asociada con un ID de usuario y es almacenada.

La plantilla de la huella almacenada se utiliza para compararla con el dedo que el usuario coloco, esta plantilla de huella es usada para identificar la identidad del usuario, así que un usuario enrolado es apto para checar en el equipo, todo este procedimiento toma alrededor de dos segundos, para el mismo número de ID hay hasta diez diferentes huellas que puede enrolar, asi el usuario podría tener mas formas de verificación.

Idealmente cada dedo de cada mano debería de ser enrolado, así si

un dedo enrolado está dañado, puede alternar a una de las huellas de respaldo que esté en condiciones normales, es recomendable que al menos dos dedos sean enrolados, por ejemplo, el índice izquierdo y derecho, así el usuario será capaz de usar cualquiera de los dos dedos para identificarse y se quitara de problemas si olvida cual de los dos dedos había registrado.

Identificación/Verificación de Usuario

El proceso de comparar el dedo puesto por el usuario con la huella almacenada en la plantilla. Cuando un usuario cualquiera pone un numero de ID o coloca un dedo en el sensor de huellas y pone una contraseña o pone la huella, después de que el proceso de verificación se lleva a cabo, el sistema le mostrara si la identificación fallo o se completó satisfactoriamente en el equipo. La verificación ocurre cuando un usuario cualquiera pone su número de ID o pone un dedo en el lector de huellas y luego ingresa la contraseña para la comparación con la plantilla almacenada.

Umbral

Umbral – Un número predefinido, a menudo controlado por el administrador del sistema biométrico, quien establece el grado de correlación necesario para que una comparación sea aceptada o rechazada. Si la puntuación resultante de la comparación con la

plantilla supera el umbral, la plantilla coincide (aunque las plantillas en si no sean idénticas).

El umbral establece un balance entre una Tasa de Aceptación Falsa (False Acceptance Rate FAR) y una Tasa de Falso Rechazo (False Rejection Rate FRR). FAR se refiere a la probabilidad que un sistema biométrico identificará incorrectamente a un individuo o fallara al rechazar a un impostor. La tasa dada normalmente asume que FRR mide la probabilidad que el sistema biométrico fallará al identificar un enrolado, o verificar la identidad declarada legitima de un enrolado.

Usted puede establecer el umbral para todos los usuarios. Para un usuario al que se le dificulta la verificación por huella, usted puede adoptar un ID y una verificación de huella (coincidencia uno a uno).

El aumento del umbral incremente la seguridad, mientras que aumenta la reducción al pasar. El balance correcto es vital. Para un usuario que su dedo esta desgastado o dañado el umbral debería ser reducido.

Aviso: FAR y FRR se afectan entre sí, si se incrementa el FAR entonces se reduce el FRR. El umbral por defecto es 35, 1:1 coincidencia de umbral es 15.

Table 1—1 Configuraciones sugeridas de umbral

FRR	FAR	Uno a muchos	Uno a uno
High	Low	45	25
Middle	Middle	35	15
Low	High	25	10

Números ID de usuarios

Antes de comenzar el enrolado de huellas, a cada usuario le es asignado un numero de ID de usuario. Este numero de ID es utilizado para llamar a la plantilla de huella o contraseña cada vez que una verificación sea requerida.
Números ID son normalmente puestos mediante el teclado, pero puede ser puesto por otros medios como una tarjeta RF, tarjeta Mifare (esto es posible ya que el equipo cuenta con lector de tarjetas)

Niveles (estado) de Privilegios

Los privilegios son los permisos de uso que se dan. Esto define la habilidad de un usuario para realizar cambios administrativos y otras tareas, incluyendo la habilidad para ver, editar, agregar o renovar categorías con información específica.

Se le llama niveles de privilegios al conjunto de permisos que pueden ser modificados según se requiera, cuatro niveles de

privilegios de usuario son asignados por el lector de huellas, estos son usuario, enrolador, administrador y súper administrador (supervisor).

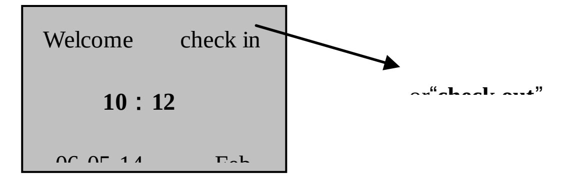
El sistema de identificación de huellas tiene cuatro estados o niveles de privilegios:

- Los usuarios son personas cuya identidad debe ser verificada, por ejemplo para tener acceso a una instalación o tener su registro de asistencia.
- Los enroladores son usuarios que están autorizados para enrolar nuevos usuarios o borrarlos del sistema.
- Los administradores pueden realizar otras tareas, excepto establecer opciones avanzadas y enrolar privilegios de administrador.
- Los supervisores son usuarios que tienen acceso a todas las funciones y pueden cambiar cualquier cosa en el sistema.

Nota: Si no hay estado de administrador o supervisor en el sistema, el enrolador deberá enrolarlos. Y si no hay un supervisor en el sistema, el administrador lo deberá enrolar.

Ventana de inicio

Presione el botón de encendido y la pantalla se iluminara, ésta es llamada la ventana de inicio. Es la siguiente figura:



Comenzando

Este capítulo describe como enrolar y verificar usuarios en un sistema de verificación de huellas.

Se incluyen los siguientes temas:

- Enrolando usuarios
- Probando un enrolado
- Enrolando una huella auxiliar de usuario
- Verificando su identidad
- Sugerencias para enrolados exitosos

Enrolando Usuarios

Después de instalar y encender su equipo lector de huellas, deberá de enrolar usuarios. Si es el primer enrolado en un sistema nuevo o vacio, todos se convertirán en enroladores, si hay un administrador en el sistema, deberá tener permiso del administrador para enrolar un nuevo usuario.

Este equipo provee tres maneras de enrolarse, como enrolado de huellas, el enrolado de contraseña y el enrolado de huella y contraseña. Estas tres maneras se adaptan a diferentes personas cuya calidad de huella es diferente. El enrolado de huella es apropiado para personas cuya calidad de huella es buena; el enrolado de huella y password son apropiados para el personal cuya

huella es enrolada exitosamente pero se le dificulta el proceso de verificación; el enrolado de contraseña es apropiado para el personal cuya huella no se puede enrolar exitosamente. De acuerdo a su situación actual, usted deberá seleccionar el enrolado mas apropiado.

Para empezar el proceso de enrolado, primero identifíquese usted mismo—presione [Menú], ponga su número de ID o huella, y así verificar su identidad。

Nota: Si es el primer enrolado en un equipo Nuevo o vacio no será necesario que se verifique.

Enrolado de Huellas

1）Presione el botón de MENU para entrar al enrolado de usuario，En la opción enrolar huella presione [OK] y aparece la siguiente pantalla:

Nota：Este lector de huellas tiene por defecto un numero de 5

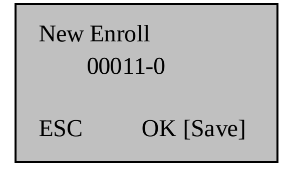
New Enroll

Enroll No 00011
ESC OK

dígitos, si el numero que necesita enrolar no es de 5 dígitos, el equipo antepondrá 0 al número para completar los 5 dígitos. Por ejemplo, si su número es el 11, en la pantalla del equipo se mostrara 00011.

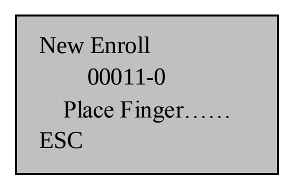
2) Digite el numero de enrolado (el rango es de 1 a 65534), presione [OK],

Aparecerá lo siguiente:



Note：00005-0
El último 0 se refiere a que es la primera huella

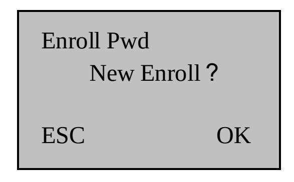
3) Si la prueba tiene éxito tres veces, aparecerá lo siguiente:



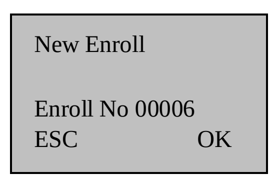
4) Presione [OK], el mensaje anterior continua mostrándose mientras la plantilla es creada. Si no se puede verificar su identidad, se le pedirá que intente de nuevo y deberá de volver a iniciar el proceso de verificación (paso 2).

Enrolado de contraseña

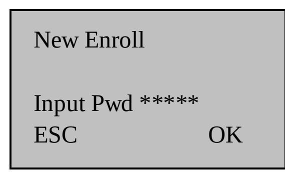
1）Presione el botón de MENU para entrar a enrolar usuarios, vaya a enrolado de contraseña, presione [OK], aparecerá lo siguiente:



2）Presione [OK], aparecerá lo siguiente:



3） Digite el número de enrolado (el rango es de 1 a 65534), presione [OK], aparecerá lo siguiente:



4）Digite su contraseña, aparecerá lo siguiente:

New Enrollment

Input Pwd ******
Pwd Affirm ******

5) Digite de nuevo la contraseña, presione [OK], aparecerá lo siguiente:

New Enroll
00006-P

ESC OK [Save]

Note：00006-P
La letra P significa password (contraseña).

6) Presione [OK], el mensaje aparecerá mientras la plantilla es creada.

Huella y contraseña

1) Presione el botón de MENU para entrar al enrolado de usuarios, Ingrese a Contraseña & Huella, presione [OK], aparecerá lo siguiente:

FP& Pwd
New Enroll？

ESC OK

2）Presione [OK], aparecerá lo siguiente:

New Enroll

Enroll No 00008
ESC OK

3）Digite la contraseña (rango de 1 a 65534), presione [OK], aparecerá lo siguiente:

New Enroll
00008-0
Please
finger……ESC

4）Si la prueba es exitosa aparecerá lo siguiente

New Enroll

Input Pwd: *****
ESC OK

:

5) Digite su contraseña, aparecerá lo siguiente:

New Enroll

Input Pwd *****
Pwd Affirm *****

6) Digite de Nuevo su contraseña, presione [OK], aparecerá lo

New Enroll
00008-0P

ESC OK [Save]

siguiente:

7) Presione [OK], el mensaje se sigue mostrando mientras la plantilla es creada.

Nota：00008-0P; el Segundo digito de derecha a izquierda es el numero de huella, La letra P significa password (contraseña).

Enrolar ID ★

1) Presione MENU para entrar a enrolar usuario, Accese a Reg RFID, presione [OK], aparecerá lo siguiente:

RFID
New Enroll？
ESC OK

2）Presione [OK], aparecerá lo siguiente:

New enroll
Enroll No: 00010
ESC OK

3） Digite el número de enrolado (el rango es 1 a 65534), presione [OK], aparecerá lo siguiente:

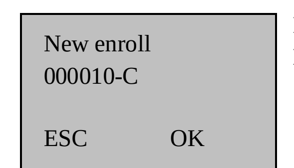
New enroll
Please show the card
Enroll No: 00010
ESC OK

4)Deslice la tarjeta cerca del equipo para que lea el ID de la tarjeta, aparecerá lo siguiente:

New Enroll
RFID：16650449
Enroll No: 00010
ESC OK

5）Presione “**OK**” para completar el enrolado. Aparecerá lo

siguiente:



Note : 00010-C
La letra C indica tarjeta ID

6) Presione 'ESC' para cancelar el Nuevo enrolado, presione OK para guardar los datos enrolados, a fin de que complete el registro de la tarjeta.

Nota : Tarjeta ID es una opción en un equipo lector de huellas, si quiere personalizar su lector de huellas con la función de tarjetas ID, por favor contacte con nuestro encargado de ventas. Si quiere mas información vaya a "Guía de uso de tarjetas ID"

Enrolar Tarjeta ID ★

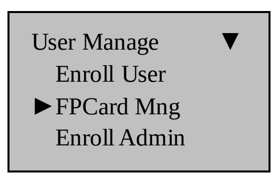
El procedimiento de esta operación es el mismo que la operación de tarjeta ID, use tarjeta HID solo si usa 125MHZ, 13.56 MHz solo con tecnología de tarjeta inteligente, estos lectores de huellas proveen usuarios con nuevas opciones que soportan multi-autenticacion de identidad. Combine una tarjeta de presentación sin contactos con un lector de huellas biométrico. O use un número de identificación personal (PIN) junto con una tarjeta de presentación sin contacto. (Vea multi-autenticación)

Una tarjeta estándar HID esta encriptada usando un formato especifico de tarjeta ID y el código del equipo.

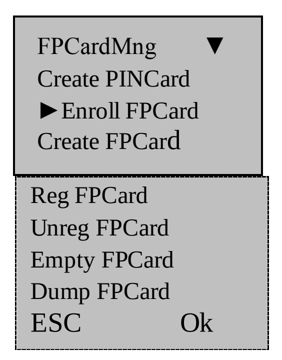
Nota：La tarjeta HID es una función opcional en el lector de huellas, si desea personalizar el lector con la función de tarjetas HID por favor contacte con nuestro encargado de ventas.

Enrolar tarjeta Mifare ★

1) Presione la tecla (MENU) en la pantalla inicial, después de que sus privilegios sean admitidos, siga la información que aparece en la pantalla:



2) Presione la tecla (ok), para entrar a las siguientes opciones:



Hay ocho submenús, como crear tarjeta de huella, enrolar huella en tarjeta, registrar tarjeta con huella, cancelar tarjeta de huella, borrar huella de tarjeta, copiar huella de tarjeta, transferir huella a tarjeta, a continuación se explicara cada uno de los submenús.

1. Crear PIN de Tarjeta (Create PIN card): Utilice un usuario registrado en el lector de huellas para crear PIN de tarjeta, el usuario deberá identificarse mediante su tarjeta y no colocar el dedo.

2. Enrolar huella en la tarjeta (Enroll FP card): la huella que ha sido almacenada la almacena directamente en la tarjeta, a partir de ahora ya hay una huella dentro de la tarjeta y ésta no existe en el equipo, el usuario podrá necesitar la "Tarjeta + Huella" para identificarse, deberá mostrar primeramente la tarjeta de huella y luego colocar el dedo.

3. Crear tarjeta de huella (Create FP Card): Copie la huella del equipo en el que existe a la tarjeta, el usuario puede usar la huella para verificarse, también puede utilizar la huella y una tarjeta de huella.

4. Registrar tarjeta de huella (Reg FP Card): Hay mas de dos equipos de asistencia, Una tarjeta PIN enrolada en un lector de huellas que quieren que se utilice en otro equipo lector de huellas, la tarjeta de huella debe registrarse primero.

5. Quitar del registro una tarjeta de huella (Unreg FP Card): Esto es el caso contrario al proceso descrito antes que este.

6. Borrar huella de una tarjeta de huella (Empty FP Card): Elimina todos los datos (huella, PIN) de la tarjeta de huellas.

7. Copiar huella de la tarjeta (Dump FP Card): Copia una huella desde la tarjeta al equipo lector de huellas, después de hacer esto

será capaz de checar directamente.

8. Transferir huella a la tarjeta (Move to FP Card): La huella en el equipo lector de huellas es transferida a la tarjeta de huella. Después de la transferencia ya no habrá huella en el equipo lector de huellas.

Nota：Tarjeta Mifare es una función opcional en los lectores de huella, si desea personalizar su equipo con la función de tarjetas Mifare por favor contacte con nuestro encargado de ventas. Si desea saber mas información lea la guía de uso de la tarjeta Mifare

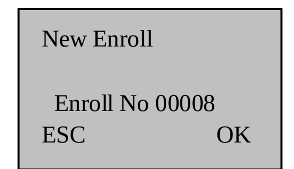
Probando un enrolado

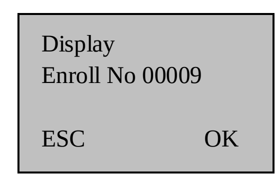
Pida a los usuarios que pongan su dedo para probar la verificación. Si la prueba es exitosa podrá empezar a enrolar huellas. Si hay calidad pobre de la huella, se le recomienda que use Huella & Contraseña.

Enrolando una huella auxiliar de usuario

Para un largo tiempo de uso, si la memoria del sistema lo permite, es mejor enrolar mas de dos huellas por usuario. Entre a la interface

de enrolar Nuevo, presione ‘OK ‘para continuar la realización de enrolar un Nuevo usuario, Presione ‘ESC’ para cancelar el enrolado nuevo y entrar a la interface de huella de respaldo, aparecerá lo siguiente:





Este procedimiento es el mismo que el de enrolar un Nuevo usuario

Nota: Cuando la memoria del sistema lo permita, es recomendable tener al menos dos dedos enrolados por usuario.

Tipo de Autenticación

Autentificación de huella

Utilice las huellas para validar la autenticación de acceso con los siguientes tipos:

（1）Autenticación 1：1（Verificación）

En este modo, ponga un ID registrado previamente y después una huella. La huella enrolada correspondiente al ID será comparada con la introducida en una base de 1:1. La autenticación 1:1 toma un

poco de tiempo independientemente del número de usuarios. No hay necesidad de hacer ninguna configuración especial en el equipo. Después de poner el ID, ponga la huella para realizar la autenticación. Diagramas de bloque de enrolado, verificación e identificación de tareas.

Procedimiento：

Coloque el dedo en la superficie del sensor, aparecerá lo siguiente:

1：1 FP Verify
Enroll No 00011
ESC OK[Pwd]

Nota :El numero por defecto de este equipo para enrolar es de 5 dígitos, si su número de enrolado no alcanza los 5 dígitos, el equipo agregara 0 al principio de su número. Ejemplo si su número es el 11, el 00011 será mostrado en la pantalla del equipo.

Presione “OK”, luego coloque el dedo en la superficie del sensor, aparecerá lo siguiente:

1：1 FP Verify
Please Move Finger

Así continuara por cerca de 0.5 segundos. Si la prueba es exitosa dirá “Gracias”, aparecerá lo siguiente:

```
FP Verify

  Enroll No 00001
    Verified！
```

Si su identidad no se puede verificar, se le pedirá que intente de nuevo, aparecerá lo siguiente:

```
FP Verify

  Place Finger Agn！
```

Así continuara por cerca de 0.5 segundos y regresara a la pantalla de inicio.

（2）Autenticación 1：N (Identificación)

Solo huellas enroladas son usadas para autenticación. Aunque el proceso de autenticación es simple, este método tomara un poco mas de tiempo que la autenticación 1:1 si hay muchos usuarios. No es necesario hacer configuraciones especiales en el sistema.

Procedimiento:

Coloque el dedo sobre la superficie del sensor, aparecerá lo siguiente:

FP Verify Please Move Finger

Esto continúa por cerca de 0.5 segundos. Si la prueba es exitosa, dirá "Gracias", aparecerá lo siguiente:

FP Verify Enroll No 00001 Verified !

Si su identidad no puede ser verificada, se le pedirá que lo intente de Nuevo, aparecerá lo siguiente:

FP Verify Place Finger Agn !

Esto continua por cerca de 0.5 segundos y regresa a la pantalla de inicio.

1: G; 1: H (Autenticación de Grupo)

Para autenticación de grupo el usuario puede definir un rango de ID de usuario, si un ID de usuario esta dentro del rango, la forma de

autenticación debería ser 1: N, de lo contrario el procedimiento de autenticación es coincidencia 1:1.

--1: Autenticación H: Usuario deberá introducir el ID para realizar la autenticación de huella, si el ID introducido es todo el ID el sistema llevara a cabo la autenticación 1:1.

--1: Autenticación G: Usuario deberá estar en un grupo antes de la autenticación, puede especificar un ID de grupo de 1-4 dígitos para cada grupo de usuarios. Deberá introducir un ID de grupo y presionar la tecla de flecha hacia abajo y luego poner la huella para la autenticación. Puede especificar un ID de grupo cuando registra un nuevo usuario. A diferencia de otros métodos deberá introducir el ID de grupo y luego presionar la tecla fleche hacia abajo antes de poner una huella para realizar la autenticación de grupo.

Autenticación de contraseña

Una contraseña de 1-5 dígitos es utilizada para validar la autenticación de acceso. Puede utilizar este método en un caso especial como cuando los lectores de huella están dañados.

Para empezar el proceso de enrolado digite su número de ID, aparecerá lo siguiente:

1：1FP Verify

Enroll No 00008
ESC OK[Pwd]

Presione [OK], aparecerá lo siguiente：

Pwd Affirm

Enroll No：00008
Input Pwd：*****

Digite la contraseña correcta y presione [OK], aparecerá lo siguiente:

Pwd Affirm

Enroll No 00008
Verified!

Si la contraseña no puede ser verificada aparecerá lo siguiente:

Pwd Affirm

Enroll No 00008
Error Pwd！

Autenticación de tarjetas RF/ MIFARE ★

La tarjeta RF de un usuario es utilizada para identificarlo. Puede registrar el número de tarjeta RF en el sistema para proporcionar protección contra robo o extravío.

Autenticación de tarjetas MIFARE ★

La tarjeta MIFARE es una tarjeta IC que no necesita tener contacto con el equipo para ser leída, la tarjeta tiene 1 K byte de memoria asignada en 16 sectores, cada uno con cuatro bloques de 16 bytes cada uno. La tarjeta MIFARE interactúa con el lector, que es capaz de almacenar plantillas de huellas dentro de él, la plantilla de la huella es transferida al lector, entonces la plantilla se compara con el dedo puesto mientras se da la verificación de rendimiento.

La tarjeta MIFARE también tiene un único numero se serie que puede usarlo en lugar del ID de tarjeta. **Para mas detalles vea al apéndice.**

Si la tarjeta Mifare ha sido usada como fue creado el PIN de tarjeta, necesita entrar ”Menú→Option→SystemOption→Advance Option”, presionar “▲/▼”, seleccionar “ Numero deTarjeta” como Y (Yes) y luego confirme todo.

En la ventana de inicio ingrese la tarjeta PIN cerca del área de inducción (la distancia no deberá ser muy grande o la tarjeta no será detectada) aparecerá la siguiente pantalla:

Verify PIN Card

UserID 00008
Verified

Si uso otra forma para registrar tarjetas Mifare (por ejemplo: El registro de tarjeta de huella), Establezca opción “No. card” como Y

(Yes), luego confirme todo.

Si estableció la opción "No. card" como N (No), entonces la confirmación será: En la interfaz inicial, (la distancia no debe ser muy grande o la tarjeta no será detectada), aparecerá una pantalla como la siguiente:

Verifying FPCard
00009
Place Finger……
Any key to Cancel

Coloque el dedo en la superficial del sensor, aparecerá lo siguiente:

Verifying FPCard
00009
Please move finger
Any key to Cancel

Sera mostrado por cerca de 0.5 segundos. Si la prueba es exitosa dirá "Gracias", aparecerá lo siguiente:

Verifying FPCard
00009
UserID 00009
Verified!

Si su identidad no puede ser verificada, se le pedirá que intente de nuevo, aparecerá la siguiente pantalla:

Verifying FPCard
00009
Please try again
Any key to cancel

Esta se seguirá mostrando por cerca de 0.5 segundos y regresara a la pantalla inicial。

Nota: Aparte del tipo de autenticación arriba mencionado, también se provee la multi-autenticacion. Vea los apéndices. Si quiere esta función por favor contacte con nuestro encargado de ventas.

Sugerencias para enrolados exitosos

Si la huella tiene una Buena calidad la velocidad de verificación será mas rápida; en caso contrario verificara mas lento u ocurrirá a FRR. Para mejorar la calidad de verificación de huellas se recomienda tomar en cuenta las siguientes sugerencias

Problema	Solución
La huella está muy seca o sucia	Solucione el problema tallando el dedo en la palma. Si la huella está seca, pruebe humedeciéndola un poco como con el roce del aire sobre él.
No es suficiente al ejercer presión	El usuario debería colocar el dedo firme y plano en la superficie del sensor.
Como seleccionar el dedo?	Es recomendado que sea el índice izquierdo o derecho o el dedo medio. Use huellas de Buena calidad, sin desgaste o daños. El usuario usualmente selecciona el dedo índice

	pero si es de mala calidad se le recomienda elegir el dedo medio o el anular. Si el dedo del usuario es pequeño deberá seleccionar el pulgar.
Como colocar un dedo?	Coloque el dedo firme y debe estar tocando por lo menos 2/3 de la superficial del sensor. La huella no debe tocar donde no es la superficie del sensor. No coloque el dedo muy rápido; No mueva el dedo mientras este en la superficie del sensor.
El efecto del cambio en el patrón de huella	Para un usuario con desgaste o daño en el dedo, la identificación puede ser afectada. Si la calidad de la huella es mala debería seleccionar una contraseña para verificarse.
Otros	Sin embargo, son pocas las personas que no se pueden verificar en el lector de huellas. Por favor use verificación de ID & Huella y el umbral puede ser reducido o use verificación por contraseña.

Enrolado de Administrador

Para prevenir que personal sin autorización cambie opciones en el equipo, éste provee una opción para establecer un administrador.

1) Entre al menú del equipo, después de que se verifique exitosamente aparecerá la siguiente pantalla:

Menú ►User Enroll Option Sys Info

2) Presione la tecla **OK,** Entre a administración de usuario, aparecerá lo siguiente:

User Enroll ►User Enroll Enroll Admin Delete Datum

3) Usando las teclas "▲/▼" seleccione enrolar administrador, aparecerá lo siguiente:

User Enroll User Enroll ►Enroll Admin Delete Datum

4) Presione la tecla **OK** Entre a la administración de enrolado y aparecerá la siguiente ventana:

Enroll Admin ►Enroll FP Enroll PWD FP&PWD

5) Puede seleccionar la forma para registrar un administrador, la

autorización de administrador incluye autorización de enrolar, autorización de administrador, y autorización de súper administrador (supervisor), para más detalles vea niveles de privilegios. La manera de enrolar es la misma que el enrolado de un usuario normal.

Borrar datos enrolados

Si desea borrar un usuario puede seguir los siguientes pasos para hacerlo.

1) Presione la tecla **Menú.** Entre al menú del equipo y después de que se verifique aparecerá lo siguiente:

Menú
►User Enroll
Option
Sys Info

2) Presione la tecla **OK,** Entre a la administración de usuarios, aparecerá lo siguiente:

User Enroll
►User Enroll
Enroll Admin
Delete Datum

3) Usando las teclas “▲/▼” seleccione enrolar usuario, aparecerá lo siguiente:

User Enroll
User Enroll
Enroll Admin
►Delete Datum

4) Presione la tecla **OK** para entrar en la opción borrar datos, aparecerá lo siguiente:

Delete Datum

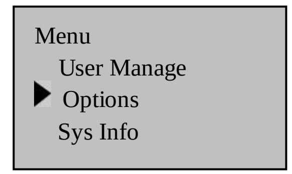
UseID 00008
ESC OK

5) Introduzca el numero que desea borrar, presione OK para confirmar y siga las instrucciones de la pantalla para borrar al usuario.

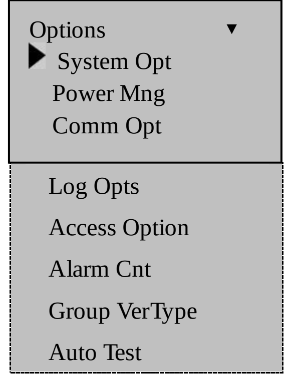
5

Opciones

Presione la tecla de [Menú] y verifique su identidad, aparecerá lo siguiente:



Vaya a Opciones, presione **[OK]**, aparecerá lo siguiente:

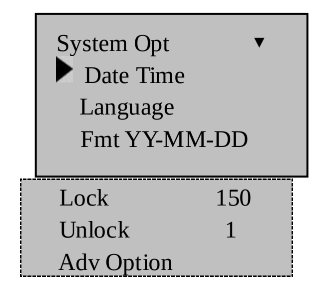


Se incluyen los siguientes puntos: Opciones de sistema, Administración de energía, Opciones de comunicación, Opciones de log, Opciones de acceso, Contador de alarmas, Tipo de verificación de grupo y Auto prueba. El contador de alarmas (Cuenta las veces que alguien fallo al verificarse) y el tipo de verificación de grupo (Verificación por tipo de grupo) son menús

opcionales, solo disponibles en equipos de control de accesos.

Opciones de sistema

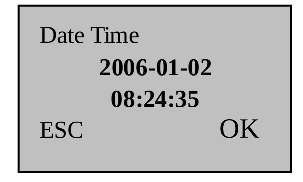
Acceda a las opciones de sistema, aparecerá lo siguiente:



La configuración de instalación abarca cuatro áreas: Opciones de sistema, Lenguaje, Bloqueos y Opciones Avanzadas.

Establecer Fecha y Hora actuales

Acceda al menú Fecha-Hora, aparecerá lo siguiente:



Para cambiar la fecha y hora presione la tecla “V” e introduzca la

fecha y hora correctas y luego presione la tecla **[OK**]

Cambiando el formato de Fecha y Hora

Acceda a la opción **Fmt YY-MM-DD**, presionando las teclas "∨" y "∧" seleccione el formato que desee, presione **[OK**]

System Option ▼
Date Time
Language
▶ Fmt YY-MM-DD

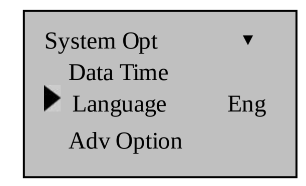
Hay diez formatos: **YY-MM-DD、YY/MM/DD、 YY.MM.DD、 MM-DD-YY 、 MM/DD/YY 、 MM.DD.YY 、 DD-MM-YY 、 DD/MM/YY、DD.MM.YY、YYYYMMDD。** Esto para cambiar el formato a mostrar de Fecha y Hora en la pantalla inicial.

Ejemplo: el formato **YY/MM/DD** (izquierda) se puede cambiar al formato **YY-MM-DD** (derecha)

Welcome check-in **17 : 37** **05/08/30** Monday	Welcome Check-in **17 : 37** **05-08-30 Monday**

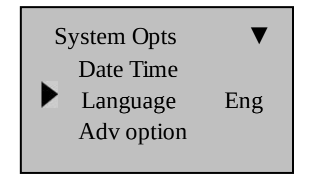
Cambiando el lenguaje

Seleccione el lenguaje que desea y presione OK, el lenguaje por defecto es Ingles; la pantalla es mostrada en ingles.

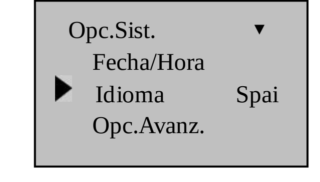


Presione la tecla hacia arriba o hacia abajo para cambiar el tipo de lenguaje, el equipo soporta varios lenguajes.

Seleccione el lenguaje que desee y presione OK, después presione ESC para salir de las opciones del sistema, el sistema le preguntara si desea guardar los cambios, confirme que desea guardar los cambios. Asegúrese de reiniciar el equipo para que los cambios tengan efecto.



Ingles



Español

Nota：Este lector de huellas no tiene como estándar la función de multi-lenguaje, si necesita esta función por favor contacte con la persona de ventas.

Bloquear ★

Este bloqueo se refiere a la duración de una cerradura, el lector de huellas controla el tiempo que podrá estar abierta una cerradura electrónica. Seleccione esta opción y presione la tecla OK para entrar a la configuración, introduzca el intervalo de tiempo con las teclas de números, presione ESC para salir y guarde la configuración.

Esta duración se mide en unidades de 20 ms, y el máximo valor de unidades es 254, que corresponde a 5.08seconds. “0” significa que estará la puerta cerrada.

Nota：Estas son configuraciones opcionales, esta opción solo viene en equipos que tienen una función de control de acceso simple. Si el equipo es específicamente de control de acceso entonces contendrá esta opción.

Los parámetros de la duración de la cerradura siguen un estándar. Si desea mas amplio el rango de valores por favor contacte con nuestro vendedor.

Desbloquear ★

Esta opción se refiere a la cantidad de personal que puede desbloquear la cerradura. Seleccione esta opción y presione la tecla OK para entrar a la configuración, introduzca el valor con las teclas numéricas, presione la tecla ESC para salir y guarde los cambios.

El valor por defecto es 1, eso significa que solo un usuario podrá abrir cuando su verificación sea positiva, si este valor fuera 3 eso significa que el equipo solo mandara la señal de apertura hasta que tres usuarios sean verificados correctamente, el intervalo entre cada persona será de 30 segundos. El máximo valor que podrá poner en esta configuración es 5.

Nota: Esta función se relaciona con la función de bloquear. Un equipo con la función de control de acceso la tendrá.

Opciones Avanzadas

Acceda a las Opciones Avanzadas y presione [OK], aparecerá lo siguiente:

```
Adv Option            ▼
▶ Restore Deflt
  Del Logs
  Clear all Data
  Clr admin pri
  Show Score
  Match Thr           45
  Only 1 to 1          N
  1:1 thr             25
  Two sensor           N
  Voice                Y
  No.Card Only         N
  R.card Only          Y
  FP Card Only         Y
  Upd firmware
  Remote Auth          Y
  Auth Server
  Work code            N
  Button Beep          Y
  AdjVol(%)           34
  Print
```

.

Presione "▲/▼" para ir de arriba a abajo de la pantalla y seleccionar la opción que desee.

- **Restaurar valores por defecto:** Restaura todas las configuraciones a los valores de fabrica.
- **Borrar todos los datos**: Borra todos los usuarios enrolados y los logs.
- **Borrar log**: Borra todos los logs de la memoria.
- **Borrar privilegios de Administrador:** Cambia los privilegios de administrador por opciones de un usuario común.
- **Mostrar resultados**: Muestra o no el valor de la calidad de huella en la pantalla.
- **Umbral:** Para ayuda en la selección del nivel de umbral vea la tabla.
- **Solo 1 a 1**: Si el numero ID del personal debe ser ingresado。
- **Umbral 1:1 :** Cuando use ID + Huella para verificarse establezca el nivel de umbral.
- **Dos sensores:** Si es necesario conectar un sensor externo adicional seleccione esta opción como "**Yes**"
  Nota: Después de conectar con el sensor de huellas asegúrese de reiniciar el equipo para que los cambios tengan efecto.
- **Sonido:** Si usa una bocina o no. Si establece esta opción como (**Yes**) el equipo emitirá un sonido por cada cosa que usted

realice, por ejemplo, después de una verificación exitosa el equipo dirá (**Gracias**), si se establece como (**No**) el equipo no emitirá ningún sonido, solo cuando la verificación sea positiva emitirá un (“**do”**), cuando la verificación sea negativa emitirá dos **(“do”)**。

- **Actualización de Firmware**: Si desea actualizar el firmware del equipo puede utilizar una memoria USB o puede conectar el equipo a la PC para llevar a cabo este proceso。

  Precaución: No deberá utilizar cualquier firmware, deberá contactar con su proveedor antes de actualizar, una actualización no correcta puede causar mal funcionamiento del equipo.

- **Número de tarjeta：** Si esta opción se establece como “Yes”, solo con el número de tarjeta podrá pasar la autenticación. Si se establece como “NO”, después de verificar la tarjeta se tendrá que verificar por huella**.**

- **Solo tarjetas registradas**：Si se establece esta opción como “Yes” primero necesitara registrar la tarjeta en el equipo; si se establece como “No”, no necesitara registrar la tarjeta**.**

- **Llave de tarjeta de huella：** Después de que se establece esta

opción el equipo lector podrá escribir la contraseña en la tarjeta que ha sido registrada.

- **Remoto**：Después de establecer esta opción como "Yes", este

  equipo podrá ser usado en modo de identificación remota.
  Hay cuatro opciones a escoger en el equipo (NL, LN NO, LO) cada uno de ellas tiene un significado diferente.

  NL, Indica que primero realizara la verificación por red y después la verificación local.

  LN, Indica que primero realizara la verificación local y luego la de red.

  NO, Indica que solo hará la verificación remota, solo la base de datos remota tiene las huellas para poder pasar la verificación.

  NL, Indica que solo hará la verificación local, el equipo tiene las huellas para pasar la verificación.

- **Servidor de Autenticación:** Se especifica la dirección IP por si hay un servidor de autenticación en la red local.

- **Work Code**：Si se establece como "Yes" el equipo preguntara

  por el work code cuando un usuario quiera autenticarse, si se establece como "NO" los usuarios tendrán una autenticación normal.

- **Beep de botón**: Indica si el equipo emitirá o no un sonido al presionar una tecla.

- **Ajustar voz:** Ajusta el volumen de la voz y de los sonidos del teclado.

- **Impresión inmediata:** Esta opción establece el Puerto RS232, cuando un usuario se verifica exitosamente el equipo exportara una señal a través del Puerto serial, si el equipo se conecta con una impresora podrá imprimir la información o verla vía hyper terminal.
  Nota: Esta función solo soporta impresoras de Puerto serial (RS232), la conexión de Puerto paralelo no es soportada, la velocidad de transmisión del equipo y la impresora deberá ser la misma. Para mas detalles vea el apéndice.

Nota：

1) **Sensor de huellas adicional** y **actualización de firmware** son validos para el lector de huellas que cuenta con USB.

2.) **Numero de tarjeta** es una opción válida para equipos que cuentan con tarjetas ID o Mifare.

3.) **Solo tarjetas registradas** y **Llave de tarjeta de huella** solo son usados en equipos con la función de tarjetas Mifare.

4.) **Servidor Remoto de Autenticación** solo es usado en equipos con sistema de identificación remota (RIS).

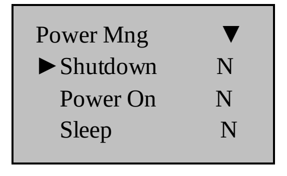
5.) **Beep de botón, Ajustar Voz** solo aplica a equipos que utilizan sensor de huellas U.are.U.

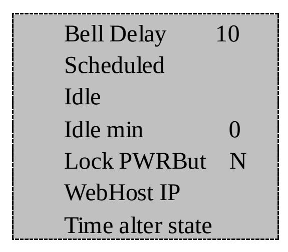
Administración de energía

Este producto utiliza un sistema de administración inteligente, soporta un interruptor de tiempo o un calendario de interruptor de tiempo, bloquea el botón de encendido de acuerdo a determinado tiempo.

Opciones de energía

Acceda al menú Administración de energía, aparecerá lo siguiente:

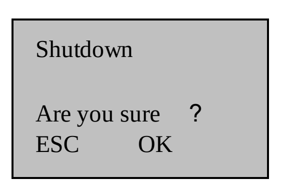




Este equipo utiliza un sistema inteligente de administración, soporta el interruptor de tiempo y funciones de inactividad, puede satisfacer las demandas del usuario.

- **Apagado:** Programar un apagado automático.

  Seleccione esta opción, presione OK y aparecerá lo siguiente:



Presione la tecla **Ok** para programar un apagado automático, presione **ESC** para cancelar.

Después de completar la programación presione OK para confirmar y que esta función tenga efecto.

- **Encendido**: Programar autoencendido;
- **Modo de espera:** Poner en modo de espera el equipo, presione cualquier tecla para regresar del modo de espera;

- **Inactivo y minuto inactivo**: Esta relacionado uno con otro, mientras el minuto inactivo sea cero, la inactividad está cerrada; mientras el minuto inactivo no sea cero, por ejemplo, si se pone un minuto, los usuarios no podrán hacer nada durante ese tiempo y el sistema se pondrá como inactivo.
- **Demora de campana (Tiempo de timbre y duración del timbre):** El sistema tiene un total de ocho campanas para programar, de acuerdo a su necesidad deberá establecer el tiempo de campana, cuando se acerque la hora de campana el equipo sonara la campana automáticamente, el sonido de la campana se detendrá automáticamente.
- **IP del servidor Web:** Establezca la dirección IP de la PC en la cual está instalado el servidor Web.
- **Ajustar volumen:** Ajusta el volumen del equipo.

- **Bloquear botón de encendido:** Establezca esta opción como (**NO**), podrá apagar el equipo presionando el botón de encendido; si establece esta opción como (**Yes**), en el menú de administración de energía aparecerá la opción de “Apagar equipo”, el equipo no se podrá apagar con el botón de encendido, deberá entrar a la opción de “Apagar equipo” para poder hacerlo.

Nota：

1.) Si no encuentra esta opción, apague el equipo, luego

enciéndalo y volverá a su funcionamiento normal.

2) La función de IP de servidor Web solo está disponible si el equipo cuenta con la opción de reproducir MP3.

3.) Tiempo de timbre y duración del timbre solo esta disponible en los equipos que tiene la función de "Tiempo de timbre y Reproductor MP3".

Condicion suplente de tiempo

Condicion suplente: Mientras se esta usando el equipo T&A, los distintos periodos de tiempo necesitan corresponder de acuerdo a la condicion de checar, el usuario puede utilizar las seis teclas para establecer la condicion de checar en el panel del equipo.

Estas teclas de condiciones se pueden establecer manualmente presionando la tecla correspondiente a la condicion que usted desea, para su conveniencia, la condición de tiempo alternativo es un elemento en el menú del equipo lector de huellas.

Condicion suplente de tiempo: Cuando se llegue la hora indicada, el equipo cambiara automáticamente la condición de checar. La actual condición de checar aparecera en la pantalla inicial del equipo.

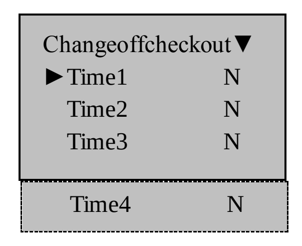
Como establecer condicion suplente de tiempo

Establecer el tiempo de la condicion suplente

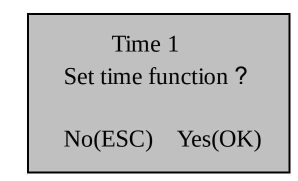
1 . Entre a **Menu - Opciones - Administracion de Energia - Condicion suplente de tiempo,** aparecera lo siguiente:

Att condition Fun
Check condition
On check-in
Exit (ESC) OK(OK)

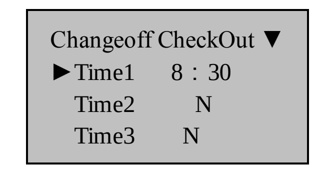
2 . Presione las teclas “▲/▼” para seleccionar la condición que desea establecer, hay cuatro opciones de condicion que puede elegir y cuatro periodos de tiempo, ellos son Checar entrada, Checar salida, Checar entrada de tiempo extra, Checar salida de tiempo extra, presione la tecla OK para establecerla, en el ejemplo se muestra “Checar salida (Check out)” :



3. Seleccione el Tiempo que desea establecer, primero seleccione el periodo de tiempo, presione la tecla OK, como se muestra:



4 . Presione la tecla OK para entrar a la siguiente pantalla, introduzca el tiempo que usted desee:



5 . Presione las teclas ▲/▼ para seleccionar otro Tiempo.

6 . Despues de completar la configuración, presione la tecla ESC para salir, la siguiente pantalla aparecera, presione OK para guardar y luego ESC para salir.

Change off check out
Save？

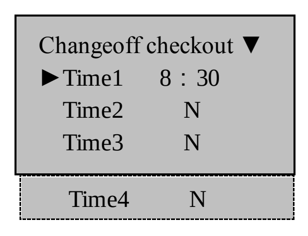
Invalid(ESC) Yes(OK)

7 . Si esta configuración se guarda cuando se llegue la hora la condición de checar se cambiará.

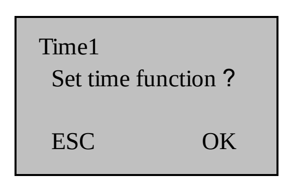
Cancelar el tiempo de establecer condicion suplente

1. Entre a establecer condicion suplente para cancelar la configuracion de "Check out"

   Entre en menu –> opciones de encendido—>condicion suplente de tiempo, elija "Check out" como se muestra a continuación:



2. Seleccione el Tiempo que desea cancelar, en el ejemplo se tomo el Tiempo 1. Presione la tecla Ok como en la figura:



3. Presione **ESC** para cancelar.

Changeoff checkout ▼
►Time1 N
Time2 N
Time3 N
Time4 N

4．Despues de terminar las configuraciones, presione la tecla ESC para salir, presione Ok para guardar y ESC para salir

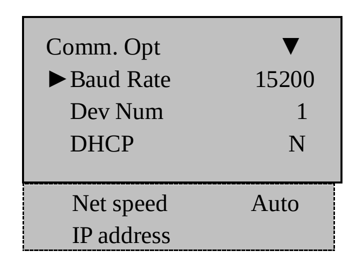
Chg off check-out
Save？

No(ESC) Yes(OK)

5．Si se guardan los cambios se cancelara el “Tiempo 1” de “Check out”

Opciones de comunicación

Acceda a las opciones de comunicacion, aparecera lo siguiente:



Net Mask	
Gateway	
TCP/IP	Y
RS232	N
RS485	N
Link code	0
ExternModem	Y

El equipo soporta **RS232, RS485, TCP/IP,** Si el equipo esta conectado como una sola unidad o en una red, podra satisfacer las necesidades del usuario.

- **Velocidad de comunicacion:** Hay 5 opciones: 9600, 19200 38400, 57600 115200;

- **Numero de equipo**: ID del equipo, el rango es de **1** a **255** ;

- **DHCP (Dynamic Host Configuration Protocol):** Activa la function de DHCP en el equipo.

- **Direccion IP:** Por defecto tiene la direccion 192.168.1.201 ;

- **Velocidad de Red:** La velocidad por defecto es Auto, tiene como opciones 10M-F, 10M-H, 100M-F, 100M-H ;

- **Mascara de Red**: La mascara de red por defecto es 255.255.255.0, la puede cambiar si asi lo requiere;

- **Gateway:** El gateway por defecto es 192.168.1.1 ;

- **Ethernet**: Establecer si usa o no el protocolo TCP/IP ;

- **RS232:** Establecer si usa o no el puerto RS232 ;

- **RS485:** Establecer si usa o no el puerto RS485 ;

- **Codigo de Link:** Por defecto viene como 0, pero puede ser cambiado.

- **Modem externo:** Se establece como Y(Yes) para que el equipo se pueda conectar a un modem adicional.

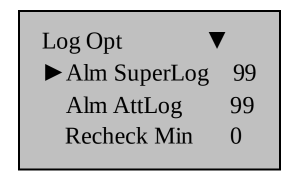
Nota :

1) Si el equipo esta provisto con un “Getaway” y una “Sub mask”, la opcion de ” Ethernet” no estara disponible, por defecto se establece como “Yes”; Si no se le asigna un “Getaway” ni una “Sub mask”, la opcoin “Ethernet” se mostrara y la podrá establecer como usted desee.

2) Despues de realizar cambios asegurese de reiniciar el equipo para que los cambios tengan efecto.

Opciones de Log

Accese a las opcoines de Log, aparecera el siguiente mensaje :



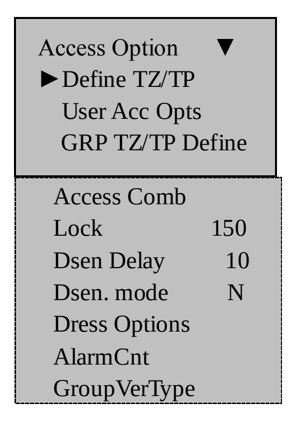
- **Log para supervisor alarmas**: cuando se llegue al limite automaticamente emitira un sonido para avisar que el log esta lleno.
- **Log de alarmas de asistencia**: Cuando se llegue al limite automaticamente emitira un sonido para avisar que esta lleno.
- **Minutos de re-chequeo**: Establezca esta opcion en minutos. Si alguien ya checo, a partir de esa hora mas los minutos que aqui establezca, si la persona vuelve a checar no sera mostrado en el sistema.

Opciones de control de acceso★

Si el equipo es provisto con una function professional de Control de Acceso esta opcion estara disponible. Esta opción no esta disponible en los equipos con funciones simples de Control

de Acceso.

Entre a opciones de acceso y presione [OK], aparecera lo siguiente:



Funciones principales en Opciones de Acceso：

- **Definir TZ**: Es la definicion del periodo de tiempo de cada dia para abrir una puerta durante una semana；
- **Opcion de Acceso a Usuarios:** Es la definicion de Grupo de usuarios, periodo de tiempo de usuarios y combinación de apertura；

- **Periodo de tiempo de grupo**: Es utilizado para establecer el tiempo de apertura para un grupo;
- **Combinacion de Acceso** (Combinacion de apertura**)**: Define diferentes combinaciones de desbloqueo, cada combinación se compone de distintos grupos；
- **Bloqueo** (Duracion de tiempo de la cerradura**)**: El equipo puede controlar el tiempo de apertura de una cerradura electrica.
- **Retraso de sensor de puerta** Es el tiempo que transcurre a partir de que se abre la puerta para que el equipo emita una alarma;
- **Modo de sensor de puerta** Hay tres opciones: Ninguno (NONE), Normalmente Abierto (NO), Normalmente cerrado (NC). Ninguno significa que no hay ningun sensor de puerta, Normalmente abierto significa que la puerta se encuentra abierta en condiciones normales, Normalmente cerrado es cuando la puerta esta comúnmente cerrada.
- **Opcion de alarma de coaccion:** Si la huella registrada es autenticada el sistema enviara una alarma automaticamente para anunciar que alguien ha sido forzado a abrir la puerta.
- **Contador de alarmas** (la cantidad de fallas al verificar)**,** si alguien falla en su verificacion las mismas veces que las de este valor el equipo enviara una alarma.

- **Tipo de verificación de grupo:** Esto significa que un usuario que pertenezca al grupo use el tipo de verificación.

Nota：Esta opción es un elemento opcional del menu. Solo algunos equipos de control de acceso la tienen, si la opcion se establece como Y(yes), el equipo será capaz de hacer la verificación de varias maneras.

Introduccion breve a las opciones de acceso

La función de opciones de acceso son las configuraciones del tiempo de apertura para usuarios registrados y la combinacion de apertura.

Cada atributo de usuario se define por el grupo al cual pertenece, use el periodo de tiempo de grupo y el periodo de tiempo de usuario. El agrupamiento es para dividir los usuarios en distintos grupos, como grupo1, grupo2, etc. Cada grupo incluye tres periodos de tiempo que son llamados periodos de tiempo de grupo, dentro de este periodo el usuario puede seleccionar 3 periodos de tiempo de los que ya están establecidos. La relación entre estos tres periodos se da mediante un “OR” (ej. Solo es necesario que se cumpla uno de estos tres periodos). En el periodo de tiempo, el usuario puede seleccionar 3 periodos de tiempo de los que ya están establecidos. La relacoin entre ellos también es mediante un “OR”.

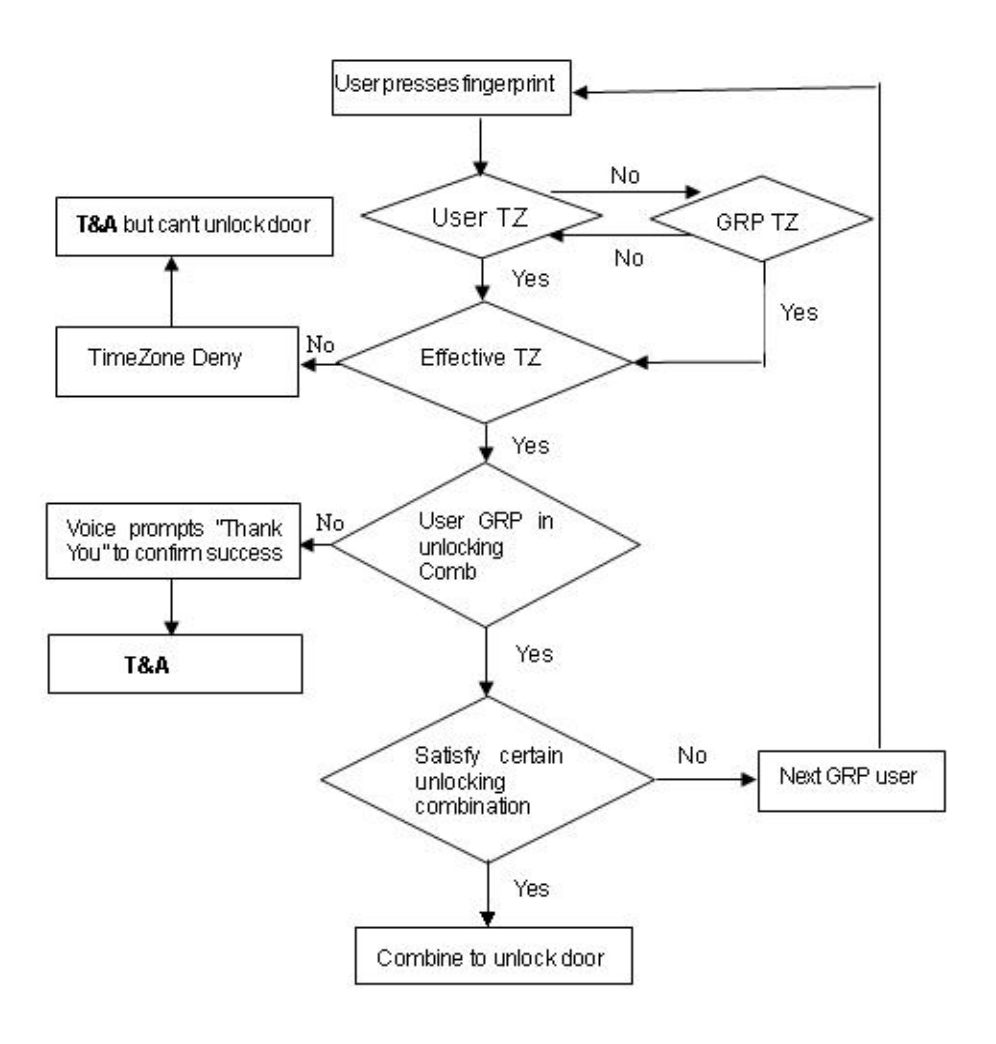
En pocas palabras, las condiciones en las cuales los usuarios registrados pueden abrir la puerta son:

1: El grupo al que el usuario pertenece se encuentra en la combinacion de apertura (este grupo también se puede encontrar en la combinacion de desbloqueo con otros grupos, pero serán necesarios los dos para abrir la puerta).

2: El tiempo actual de apertura se encuentra dentro de un periodo efectivo de tiempo.

Por defecto en el sistema los nuevos usuarios pertenecen al grupo 1, por defecto la combinación de agrupacion es grupo 1 y el periodo de tiempo de grupo es "1". Bajo la condición de que el grupo 1 y el periodo de tiempo 1 se encuentran en los valores por defecto, los nuevos usuarios por defecto se encontraran desbloqueados (si un usuario cambia la configuración de Opciones de Acceso el sistema cambiara de acuerdo a los cambios del usuario). Si el agrupamiento al que el usuario pertenece no esta incluido en la configuración de combinación de agrupamiento, el usuario solo podra registrar su asistencia pero no podra abrir la puerta.

Verificacion de opciones de flujo de acceso



Descripcion de Funciones

Definicion de periodo de tiempo

El Periodo de Tiempo es la unidad minima de periodo de tiempo de las opciones de acceso. Todo el sistema puede ser definido con un máximo de 50 periodos de tiempo y se pueden establecer 7 regiones de tiempo en cada periodo de tiempo (ej. Una semana). Cada región de tiempo es un periodo de tiempo efectivo en 24 horas al dia. Cada usuario puede tener máximo 3 periodos de tiempo. La relación entre estos tres periodos es por medio de un “OR”. Es valido siempre y cuando uno de estos tres periodos se cumpla. Cada periodo de tiempo tiene como formato de hora HH:MM-HH:MM y se basa en un sistema de 24-horas con sus respectivos minutos. Esta opcion solo se puede configurar con un Administrador o un Super Administrador.

Si el tiempo de terminación es menos que el de inicio (Ej. 23:57-23:56) significa que será de un dia a otro. Si el tiempo de terminación es mas que el tiempo de inicio (Ej. 00:00- 23:59) solo tendrá efecto en ese rango de tiempo.

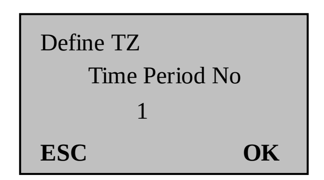
Tiempo efectivo para que un usuario abra: abierto todo el dia (00:00-23:59) o el tiempo de terminación mas grande que el tiempo de inicio en el periodo de tiempo.

Nota: Los valores por defecto del periodo de tiempo del

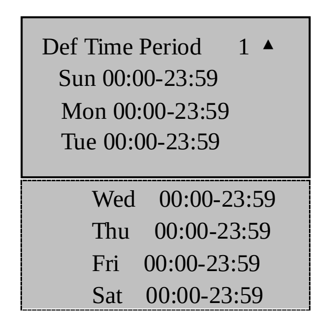
numero de serie 1 es abierto todo el dia, el Nuevo usuario registrado pertenece al grupo 1 y tendrá el periodo de tiempo del numero de serie 1, asi pues, el nuevo usuario podrá abrir puertas.

El procedimiento de configuración del periodo de tiempo es el siguiente:

1) Entre a “Definir TZ” y se mostrara lo siguiente en la pantalla:



Presione “OK” para entrar a la configuracion del periodo de tiempo 1, aparecera lo siguiente:



La definición del periodo de tiempo 1 es todo el dia abierto, ej. El valor por defecto de fabrica.

2) Por ejemplo: El periodo de tiempo puede ser redefinido.

Ej: La definicion del periodo de tiempo 1 es:
Sabado y Domingo son descanso y no se permite entrar.
En hora de trabajo de Lunes a Viernes se permite entrar.
Horario de trabajo: 08:30-18:00
La configuración quedaría como sigue:

Def Time Period	1 ▲
Sun	23:57-23:56
Mon	08:30-18:00
Tue	08:30-18:00
Wed	08:30-18:00
Tue	08:30-18:00
Fri	08:30-18:00
Sat	23:57-23:56

Multiples periodos de tiempo pueden ser definidos de acuerdo a como sea requerido en la practica. El sistema puede definir un máximo de 50 periodos de tiempo.

Definicion de función de agrupamiento

Un grupo de acceso permite a los usuarios un acceso estándar a su lugar de trabajo. Departamentos diferentes pueden tener diferentes privilegios de acceso y algunos empleados de corporaciones tienen diferentes funciones y pueden necesitar diferentes niveles de acceso para cada funcion dependiendo de sus horas de entrada y salida del

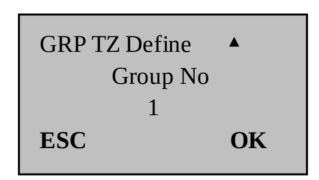
lugar de trabajo. Para agilizar el proceso de otorgar privilegios de acceso se puede hacer por grupos, en lugar de individualmente para simplificar el proceso y tener más transparencia.

Agrupar funciones puede dividir usuarios en grupos y puede tambien combinar diferentes grupos en diferentes combinaciones de acceso; la funcion de agrupamiento puede combinar varias combinaciones de acceso. El sistema es capaz de definir 5 grupos: grupo 1, grupo 2, grupo 3, grupo 4 y grupo 5. Los nuevos usuarios por defecto pertenecen al grupo 1 y usan el periodo de tiempo de ese grupo, pero pueden ser puestos en otro grupo, seleccionar el numero de serie del periodo de tiempo que actualmente esta en ese grupo. Cada usuario asignado a un grupo por defecto se le asigna el periodo de tiempo de dicho grupo, asi que es recomendable primeramente realizar la asignación de periodos de tiempo a los grupos.

Nota: Por defecto los usuarios que pertenezcan al grupo uno podrán abrir puertas.

El procedimiento para configurar el Grupo de Acceso es el siguiente:

1) Entre a “GRP 1 TZ Define ” y se mostrara lo siguiente:
2) Presione **OK** para entrar.



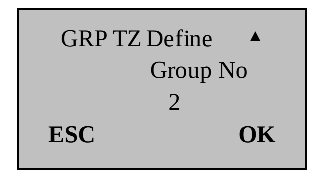
3) Hay 3 periodos de tiempo en GRP TZ Define. Las relaciones entre estos 3 periodos de tiempo son mediante un “OR”.

GRP 1Delt TZ ▲	
TZ1	1
TZ2	8
TZ3	40

4) El grupo 1 tiene periodos de tiempo efectivos de 1, 8 y 40; también se pueden definir otros periodos de tiempo.

Entre a “GRP 2 Dflt TZ ” y se mostrara lo siguiente:

5) Establezca el periodo de tiempo del grupo 2:



6) Presione OK para entrar.
El grupo 2 tiene periodos de tiempo efectivos de 2, 10 y 36; también se pueden definir otros periodos de tiempo.

GRP Dflt TZ ▲	
TZ1	2
TZ2	10
TZ3	36

7) Analizando esto, los periodos de tiempo de cada grupo pueden definirse de acuerdo a las necesidades. El sistema puede

definir periodos de tiempo de un máximo de 5 grupos.

Opciones de acceso a usuarios

Las opciones de acceso a usuario se dan de acuerdo a los requerimientos del usuario, se incluye: Para pertenecer a la configuración de agrupamiento, utilice periodo de tiempo de grupo y periodo de tiempo de usuario.

Entre a este menú para el estado de las Opciones de Acceso.

- **Agrupamiento**: divide los usuarios registrados en distintos grupos, es fácil y tiene una mejor administracion.
- **Usar GRP TZs** (Usar periodo de tiempo de grupo): si el usuario usa el periodo de tiempo por defecto o pertenece a un grupo.
- **Periodo de tiempo de usuario**: se usa para establecer el periodo de tiempo de apertura de usuario y seleccionar el numero de serie del periodo de tiempo que actualmente se establecerá.

Nota:

Relaciones entre usar periodo de tiempo y periodo de tiempo de usuario.

Yes y **No** en “**Usar periodo de tiempo de grupo**” solo afecta

el siguiente **periodo de tiempo de usuario**:

Si el **periodo de tiempo de grupo** es "**Yes**", entonces al periodo de tiempo de usuario le sera asignado automaticamente el valor del numero de serie del periodo de tiempo del grupo al que pertenece (de antemano se debe de establecer el periodo de tiempo de grupo).

Si el **Periodo de tiempo de usuario** es cambiado, entonces **Usar periodo de tiempo de grupo** cambiara automáticamente a "**No**".

El siguiente ejemplo es para ditribuir al usuario 00001 y 00002 al grupo 1 y grupo 2

A. Introduzca el numero de serie 00001 y aparecera lo siguiente:

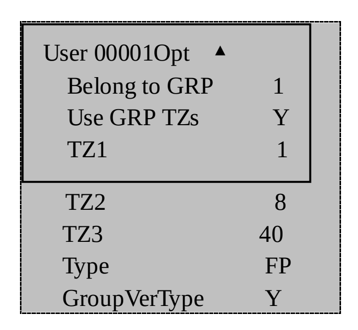
User Acc Opts ▲	
Enroll ID :	00001
ESC	**OK**

Presiopne "**OK**" para entrar al menu de **Uso de periodo de tiempo de grupo**. Presione las teclas "Arriba" y "Abajo" y seleccione "**Yes**".

Usuario 00001 esta en periodos de tiempo efectivos de 1, 8 y 48 ;

"Permitir Grupo" se establece como Yes, supongamos que el tipo de verificacion del grupo 1 es por contraseña (capacidad de establecer bajo **Tipo de verificación de grupo** de **Opcion de control de acceso)**

aparecerá lo siguiente:

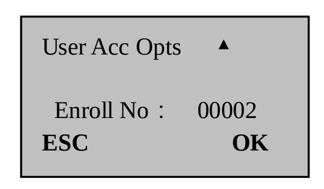


El usuario del numero de serie 00001：

1）El usuario pertenece al agrupamiento "1",utilize el periodo de tiempo del grupo 1 (el numero de usuario del "periodo de tiempo de usuario" es el numero de serie del "periodo de tiempo de grupo")；

El usuario utiliza "Tipo de verificacion de grupo", a pesar de que el usuario haya escogido cualquier tipo de verificación individual; todos tienen el tipo de verificación del grupo.

B. Introduzca el numero de serie 00002, y aparecerá lo siguiente:



Presione **OK** para entrar.

Si el numero de serie del periodo de tiempo de usuario es 1 o 20, entonces el **uso de periodo de tiempo de grupo** automaticamente cambiara a “**No**”.

Tipo de Verificacion de Grupo se establece como NO , asi el usuario puede utilizar el tipo de verificación individual como se muestra en la figura.

User 00002Opt ▲	
Belong to GRP	2
User GRP TZs	N
TZ1	1
TZ 2	20
TZ3	
Type	FP
GroupVer type	N

El usuario del numero de serie 00002：

1) El usario pertenece al agrupamiento “2”, utiliza el periodo de tiempo de usuario y no el periodo de tiempo de grupo, Ej. Tiene efecto en periodos de tiempo de 1 y 20.
Cuando el usuario quiera utilizar el periodo de tiempo de grupo debe seleccionar “**Yes**”. En periodo de tiempo de usuario el numero de serie del periodo de tiempo de grupo se le asignara

automaticamente el valor del numero de serie del periodo de tiempo de grupo. En caso contrario, si el usuario quiere utilizar el periodo de tiempo de usuario, modifique directamente el numero de serie en el periodo de tiempo de usuario y **uso de periodo de tiempo** cambiara automaticamente a “**No**”.

2) El usuario utiliza tipo de verificación individual, también llamado tipo de verificación de huella.

Combinacion de Acceso

La Combionacion de apertura es la representación directa del control de apertura. Ej. Si el usuario quiere que todos los usuarios registrados no puedan abrir, entonces podra establecer todas las 10 combinaciones de apertura como nulas.

La combinación de apertura es para definir diferentes combinaciones de apertura y cada combinacion se compone de diferentes grupos. La combinación directa de apertura usa el numero de grupo y no considera la secuencia de verificación entre cada grupo. Por ejemplo “123” representa al grupo 1, grupo 2 y grupo 3 y si al menos un usuario en cada grupo pasa la verificación entonces la puerta puede ser abierta. “4” representa que despues de que el usuario en el grupo 4 pase la verificacion la puerta sera abierta. El sistema puede definir simultáneamente un máximo de 10 combinaciones de apertura. Se requiere que solo una pase la verificacion.

Nota:

Combinacion de apertura por defecto en el sistema es "1" (ej. Los nuevos usuarios podrán abrir puertas).

El procedimiento para establecer la Combinacion de acceso es el siguiente:

Presione "MENU" y entre a la pantalla principal.
Seleccione "Options" y presione "OK" para entrar al menu de configuraciones.
Seleccione "Opciones de Acceso" y presione OK para entrar al menu.
Seleccione "Definir combinacion de apertura" para entrar "Combinacion de apertura" y aparecera lo siguiente:

Access Comb ▲	
Comb 1	1
Comb 2	
Comb 3	
Comb 4	
Comb 5	
Comb 6	
Comb 7	
Comb 8	
Comb 9	
Comb 10	

Cuando se tienen los valores de fabrica el sistema por defecto tiene que el grupo 1 esta en la combinación de apertura 1y los demás son nulos.

Si no desea que los usuarios abran la puerta, establezca las diez combinaciones de apertura como nulas.

Si solo desea que algunos grupos abran la puerta juntos, establezca estos grupos en la definicion de combinacin de apertura:

Por ejemplo:

Access Comb ▲	
Comb1	123
Comb2	4
Comb3	24
Comb 4	45
Comb 5	15
Comb 6	
Comb 7	
Comb 8	
Comb 9	
Comb 10	

De las configuraciones de arriba se puede observar que:

123 es una combinacion.

4 es una combinacion.

24 es una combinacion.

45 es una combinacion.

15 es una combinación.

Combinacion 1: cuando personal del grupo 1, grupo 2 y grupo 3 estan presentes al mismo tiempo y el periodo de tiempo es efectivo si al menos un usuario de cada grupo pasa la verificacion, entonces

la puerta se podra abrir.

Combinacion 2: solo una persona del personal del grupo 4 esta en ese momento, la puerta puede ser abierta.

Combinacion 3: cuando personal del grupo 2 y 4 se encuentran en escena y el periodo de tiempo es valido si al menos un usuario de cada grupo pasa la verificacion, la puerta podra abrirse.

Combinacion 4: cuando todo el personal del grupo 4 y 5 estan en escena y el periodo de tiempo es valido si al menos un usuario de cada grupo pasa la verificacion, la puerta podra abrirse.

Combinacion 5: cuando todo el personal del grupo 1 y 5 esta en escena y el periodo de tiempo es valido si al menos un usuario de cada grupo pasa la verificacion, la puerta podra abrirse.

Nota:

Periodos de tiempo que no pueden pasar la verificacion

- ✧ **Periodo de tiempo de usuario no seleciona numero de serie de periodo de tiempo.**
- ✧ **Periodo de tiempo de grupo no selecciona numero de serie de periodo de tiempo.**
- ✧ **Tiempo en el que el usuario pasa la verificación no incluye ningún periodo de tiempo que establece el usuario.**
- ✧ **Periodo de tiempo esta definido como prohibido.**

Si el periodo de tiempo que el usuario establece no puede pasar la verificacion.

- ✧ **Cuando se cumpla la combinación 2, el usuario que le aparezca "Tiempo invalido de periodo de acceso" no puede abrir la puerta, pero puede grabar la asistencia. (si hay un usuario en el grupo 4 que cumpla con la condicion de apertura, entonces la combinacion 2 puede abrir la puerta)**
- ✧ **Cuando se cumpla la combinación 1,3,4 y 5, el usuario que le aparezca "Tiempo invalido de periodo de acceso" no podrá abrir la puerta, pero puede grabar su asistencia**

2)Por ejemplo: una boveda bancaria require que 3 personas esten al mismo tiempo para poder abrir la puerta. La configuración quedaría como sigue:

Estas 3 personas pertenecen al grupo 2, grupo 4 y grupo 5, respectivamente y tienen el derecho de abrir la puerta en el mismo periodo de tiempo. Seleccione el grupo 1 y presione "OK" para entrar a editar el estado. Presione las teclas numéricas para introducir 245. Luego presione ESC para salir y guarde la configuracion.

Nota: Cuando la combinación 245 sea definida, el usuario no podrá definir como combinaciones 24, 25 ni 45.

Bloqueo

El bloqueo se refiere a la duración de la cerradura, el sistema require que establezca el equipo para controlar el tiempo de apertura de la crradura electrica, establezcalo como "0" si estara cerrado. Cierre la funcion de control de cerradura. La unidad de medida es de 20ms; el valor máximo puede ser 254 unidades, equivalente a 5.08s. Seleccione este elemento y presione "OK" para entrar a las opciones. Despues presione las teclas de números para introducir los digitos correspondientes. Finalmente presione "ESC" para salir y guarde los cambios.

Retraso de sensor de puerta

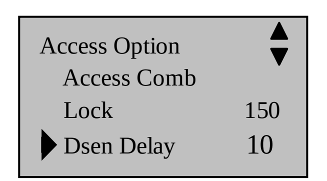
Retraso de sensor de puerta: El tiempo que deberá transcurrir después de abrir la puerta para hacer sonar una alarma;

Presione "MENU" para entrar a la pantalla principal;

Seleccione "Opciones" , Presione "OK" para entrar;

Seleccione "Opciones de Acceso" , presione OK para entrar al menú;

Presione las teclas ARRIBA o ABAJO para entrar, seleccione Retardo de sensor de puerta, aparecerá lo siguiente;



Presione **OK,** seleccione el numero, presione ARRIBA o ABAJO para modificar el Retardo de sensor de puerta.

Modo de sensor de puerta

Modo de sensor de puerta incluye 3 opciones: **No**、**NC**、**None** ;

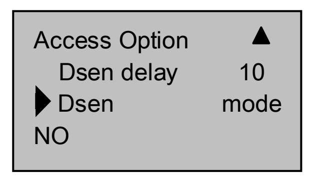
None: No se usa sensor de puerta; **NO:** Cuando la puerta esta normalmente abierta; **NC:** Cuando la puerta esta normalmente cerrada.

Presione “MENU” y entre a la pantalla principal;

Seleccione “Opciones” , presione “OK” para entrar;

Seleccione “Opciones de Acceso” , presione “OK” para entrar;

Presione las teclas ARRIBA o ABAJO y seleccione “Modo de sensor de puerta”, aparecerá lo siguiente:



Presione **OK** , seleccione la opcion, presione las teclas ARRIBA o ABAJO para cambiar la condicoin del Modo de sensor de puerta.

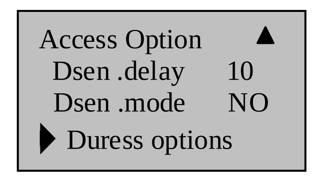
Opciones de coaccion

Presione la tecla “MENU” para entrar a la pantalla principal;

Escoja "Opciones”, presione la tecla “OK” para entrar a las opciones del Menu

Seleccione “Opciones de Acceso” , presione OK para entrar en ese Menu;

Presione las teclas “▲” y “▼” para desplazarse y seleccionar la opción:

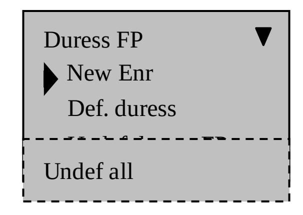


La opción de Alarma de coaccion incluye la administracion de la huella de coaccion. Busqueda de ayuda por tecla, alarma por validar 1:1, alarma por validar 1:N, alarma por verificación de contraseña y retardo de alarma.

Administracion de la huella de coacción

Use un registro Nuevo para enrolar la huella o defina una huella enrolada como huella de coaccion, el sistema enviara una señal de alarma cuando esta huella haya sido autenticada.

Acceda a la opción de alarma de coaccion, presione las teclas "▲" y "▼" para desplazarse y seleccionar "Duress FP (Huella de coaccion) ", presione "OK" para acceder:



Nuevo enrolado de huella de coaccion (New Enr.): Enrole la nueva huella como huella de coaccion.

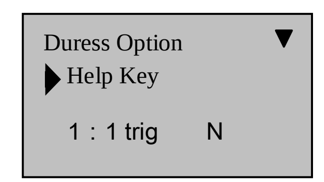
Definir la huella de coaccion (Def.duress): Cambie una huella enrolada a una huella de coaccion.

Cancelar la huella de coaccion (Undef duress FP): Cancela solamente una huella de coaccion.

Cancelar todo (Undef all) **:** Cancela todas las huellas de coaccion

Tecla de ayuda

Entre a las opciones de alarma de coaccion, presione ARRIBA o ABAJO para desplazarse y elegir “Tecla de ayuda (Help key)”



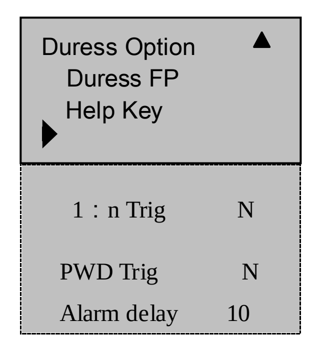
Si la búsqueda de ayuda por tecla (help key) esta definida como “y”. Mantenga presionada la tecla “▼” (mas de 3 segundos), el equipo mandara la señal; mantenga presionada la tecla “▼”(no mas de 3 segundos) y coloque el dedo o introduzca el numero de ID, despúes de la autenticación positiva el equipo mandara la señal de alarma. Si la tecla de ayuda se establece como “N”, entonces no ocurrirá nada cuando presione la tecla “▼”.

El modo de validación de alarma

El equipo soporta tres modos de verificacion:

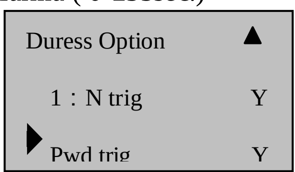
Coincidencia **1:1**, coincidencia **1: N**, **Autenticacion por contraseña**, aqui podra seleccionar una u otra forma de identificacion para la alarma de coaccion, cuando el usuario establezca la opcion como Yes, el equipo producirá una señal de

alarma



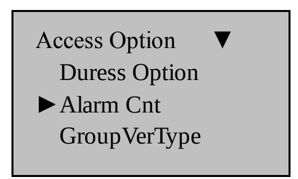
Retraso de alarma

Define un tiempo automatico: Cuando se active la alarma de coaccion el sistema no mandara inmediatamente la señal de alarma, pero puede establecer un periodo de tiempo en el que el sistema tardara en mandar la alarma (0-255sec.)



Como establecer la cantidad de equivocaciones para verificar

Esta opción es un elemento opcional, solo disponible en los equipos de control de acceso, si el usuario se equivoca tantas veces como el valor establecido el equipo mandara una señal de alarma, la configuración es la siguiente:



- Presione (MENU) para entrar a la pantalla inicial.
- Seleccione “Opciones” y presione “OK”, Presione “▲“ y “▼“ para desplazarse y seleccionar **Conteo de alarmas**.
- Presione OK e introduzca el valor que desee, el sistema soporta de 0-9 digitos para seleccionar, 0 significa que la funcion es invalida.
- Presione la tecla **OK** y salga

Tipo de grupo de verificacion

Esta opción también es un elemento opcional. Solo la tienen ciertos

lectores de huella y controles de acceso, si se establece como Y(yes), el equipo será capaz de realizar multicombinaciones para verificar, puede establecerce de la siguiente manera.

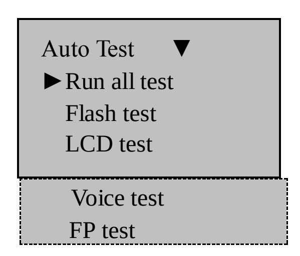
Presione “OK”, Presione “▲“ y “▼“ para desplazarse y seleccionar Tipo de verificacion de Grupo (Group VerType), se mostrara lo siguiente:

GroupVerType ▼
►1 FP / PW / RF
2 FP / PW / RF
4 FP / PW / RF
5 FP / PW / RF

Presione las teclas“▲/▼” para seleccionar un grupo, presione OK para accesar a esa linea, Presione“▲/▼” para seleccionar el tipo de verificación para ese grupo, cuando termine presione OK para confirmar, presione ESC para salir, el sistema le pedirá si desea guardar los cambios, presione OK para guardarlos.

Auto prueba

Acceda a Auto prueba, aparecera el siguiente mensaje:

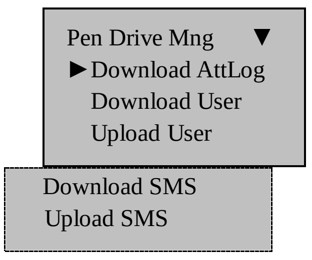


Key test
RTC test
MP3 test

En las opciones, usted puede ejecutar una prueba del sistema del equipo. Cuando el equipo esta “caido”, puede analizarlo para ver la causa de la falla del equipo y se le puede dar un mantenimiento rapido y facil. Esto prueba la **Memoria**, **LCD**, **Sonido**, **Sensor de huellas**, **teclado** y el **reloj**. En el transcurso de la prueba, deberá garantizarse la alimentación de energía; de lo contrario el sistema podria sufrir algun daño, especialmente si se esta ejecutando una prueba de memoria.

Como administrar un USB

Seleccione la administración de USB en el menú, presione[OK], aparecera lo siguiente:



El USB se puede utilizar para descargar los datos de asistencia, para descargar o subir datos de los empleados y para SMS.

Descargar los datos de asistencia

1) Conecte el USB al equipo

2) Presione MENU para entrar al menu “Administracion de USB”, Presione las teclas “▲“ y “▼“ para seleccionar “Descargar registro de Asistencia”

PenDrive Mng ▼
►Download AttLog
Download User
Upload User

3)Presione “OK” para empezar la descarga, cuando ésta haya terminado mostrara lo siguiente.

Copy data successfully！

4) Presione"ESC" para regresar a la pantalla inicial, retire el USB, los archivos X_attlog.dat (registro de asistencia), X_oplog .dat (registro de administracion), y X_user seran grabados en la memoria USB (la X se refiere al numero del equipo.

Nota: Se mostrara “copia de datos exitosa” cuando haya terminado la descarga. Si indica “No USB Disk” por favor inserte el USB e intente de nuevo.

Descargar los datos del personal

Este proceso es similar al realizado con los datos de asistencia, el archivo de user.data (datos de usuario) y Template.data(plantillas de huellas) serán grabados en la memoria USB. Estos archivos son subidos y descargados al mismo tiempo; se mostrara “copia de datos exitosa” cuando haya terminado. Si se muestra “NO USB Disk” por favor inserte el USB y e intente de nuevo.

Subir datos del personal

Seleccione “Administracion de Pendrive (USB)”. Presione “▲“ y “▼“ para desplazarse y seleccionar “Subir datos de usuario”, Presione OK para confirmar, los dos archivos, Userdat. Template, que se encuentran en la memoria serán “subidos” al equipo al mismo tiempo.

Descargar SMS

Este proceso es similar al de datos de asistencia, entre a **Administracion de Pendrive (USB)**, Presione “▲” y “▼” para desplazarse y seleccionar “Descargar SMS”, Presione OK para confirmar, cuando termine mostrara si se completo exitosamente.

Subir SMS

Despues de establecer los mensajes cortos (SMS) en el programa, “Programa Externo” - “Mensajes cortos”. Seleccione “Programa Externo”—“Administracion USB” — “Exportar mensajes cortos”—“Exportar SMS a memoria USB”. Despues de terminar la exportacion conecte la memoria en el equipo lector de huellas, seleccione el elemento en el equipo a través de “Menu”—“Administracion de USB (Pendrive)” — “Subir SMS”. Esto envia el SMS personalizado al equipo lector de huellas.

Nota：Estas funciones solo estan disponibles en equipos con funcion de USB. Si quiere usar estas funciones contacte con nuestro encargado de ventas.

Informacion del Sistema

A través de "Informacion del sistema" usted podrá ver toda la información del equipo, Acceda a [Menu]- "Info Sist", presione [OK], aparecerá lo siguiente:

```
Sys Info          ▼
►User Cnt      206
 FP Cnt       173
 Att Log      8046

 Admin Cnt     2
 Pwd User        30
 Super Logs      263
 Free Space Inf
 Dev Info
```

A continuación se muestra lo que significa cada opcion

- **Contador de usuarios**: La cantidad de usuarios que han sido enrolados.
- **Contador de huellas**: La cantidad de huellas.
- **Log de asistencia**: El registro de la asistencia que ha sido grabada en el sistema
- **Contador de administradores**: La cantidad de administradores que han sido registrados en el equipo.
- **Contraseña de usuario**: La cantidad de usuarios que utilizan

contraseña para autenticarse.

- **Informacion de espacio libre**: Informacion de la capacidad de la memoria.
- **Informacion del equipo**: Acerca de la información de este equipo.
- **Version de Firmware**: La versión del firmware del equipo.
- **Version de algoritmo**: La versión del algoritmo de identificación de huellas.
- **Numero de Serie**: Numero de serie del fabricante.
- **Fecha de fabricacion**: La fecha de fabricacion.
- **S Logs**: Logs de “Super administrador”.
- **Vendedor**: El fabricante de este equipo.
- **Nombre del equipo**: El nombre de este equipo.

Apagar Alarma

Esta funcion solo se encuentra el los equipos que tienen control de acceso. En la siguiente situación se podrá utilizar esta opción.

El usuario comete un error, utiliza el dedo de coaccion para verificarse, el equipo envía la alarma y podrá utilizar esta opción para apagarla.

Durante el mantenimiento y la instalación ocurre un accidente que ocasiona que el boton de anti-desmantelar (el boton que detecta que el equipo esta bien cerrado) se "suelta", el equipo mandara una alamra que indicara que ese boton esta fallando, si esto ocurre por favor arregle dicho botón, utilice la funcion "apagar alarma" para detenerla. Esto se hace de la siguiente manera:

Presione (MENU) para entrar a la pantalla principal.

● Seleccione la opcion "Relieve" (apagar).

●Presione▼ y ▲ para establecer el valor que desea.

Menu
Sys Info
PenDriv Mng
►Relieve Alarm

9

Ver registros T&A

Por defecto este equipo no viene con esta funcion, si necesita de ella por favor contacte con nuestro encargado de ventas.

Este equipo tiene una nueva funcion para anlizar los registros la cual prove la capacidad para consultar ya sea individualmente o todos los registros de asistencia.

1）La manera de consultar el registro de asistencia es:

Este equipo provee al usuario dos métodos para realizar la consulta:

- Entre en Menu->Ver registro de asistencia (view attendance record) Introduzca el numero de registro que desea consultar, presione [**OK**], para mostrar el registro de asistencia del numero que introducio. Si no introduce ningún número y la pantalla muestra “00000”, la consulta mostrara el registro de asistencia de todos.
- Despues de que el personal checa, antes que la pantalla vuelva al estado inicial (cuando muestra la hora en numeros grandes), presione la tecla Menu para consultar el registro de esta persona.

Por ejemplo：Consulta del registro de T&A del numero de ID 00014.

Ver T&A

```
00014 2006-5      1/23
27 08:30 12:10 13:20
   18:08
26 08:46 12:15 13:25
   18:23 18:55 22:20
25 08:53 12:07 13:19
   18:23
```

Consulta de la asistencia de todos:

```
                       1/380
00001 05-27 18:46:21I
00012 05-27 18:32:09I
00217 05-27 18:30:52I
00031 05-27 18:29:01I
00016 05-27 18:27:55I
00029 05-27 18:22:08I
```

2) Manera de "navegar" en el registro de asistencia

La manera de acomodarse los registros de asistencia es de acuerdo a la fecha, del mas Nuevo al mas viejo, mientras se navega por los registros puede utilizar las siguientes teclas para hacerlo:

Tecla	Funcion
▲	Muestra el contenido previo
▼	Muestra el siguiente contenido
1	Mueve un lugar a la izquierda para mostrar contenido
3	Mueve un lugar a la derecha para mostrar contenido
OK	Regresa al valor inicial por si se movio a la izquierda o

<table>
<tr><td></td><td colspan="2">derecha la pantalla</td></tr>
<tr><td>2</td><td colspan="2">Se mueve una línea hacia arriba para mostrar contenido</td></tr>
<tr><td>5</td><td colspan="2">Se mueve una línea hacia abajo para mostrar contenido</td></tr>
<tr><td>4</td><td>Cambia la forma de mostrar registros entre forma compacta/forma completa.
Por ejemplo en las figuras de la derecha esta la forma compacta y la forma completa del “registro completo de asistencia”.
● Forma compacta: esta diseñada para mostrar la informacion necesaria en la pantalla.
● Forma completa: esta diseñada para mostrar toda la informacion de los registros</td><td>1/380
00001 05-27 18:46:21I
00012 05-27 18:32:09I
00217 05-27 18:30:52I
00031 05-27 18:29:01I
00016 05-27 18:27:55I
00029 05-27 18:22:08I
La forma compacta
1/380
00001 27 18:46IF
00012 27 18:32IF
00217 27 18:30IF
00031 27 18:29IF
00016 27 18:27IF
00029 27 18:22IF
La forma completa</td></tr>
</table>

Ver T&A

6	Alternar entre el tamaño de la fuente, ya sea pequeña o grande (En el ejemplo se muestra con el registro de un solo empleado).	00014 2006-5 1/23 27 08:30 12:10 13:20 18:08 26 08:46 12:15 13:25 18:23 18:55 22:20 25 08:53 12:07 13:19 18:23 Fuente pequeña 27 08:30 12:10 13:20 18:08 26 08:46 12:15 13:25 18:23 18:55 22:20 Fuente grande
9	El registro mas nuevo	
0	El registro mas antiguo	

3）Ver registros e imprimirlos

Cuando usted mira los registros en el equipo, puede presionar la tecla OK para imprimir el contenido de la pantalla actual, a través de una terminal estos datos podrán ser vistos.

10

Mantenimiento

<u>Advertencia: No trate de dar mantenimiento al equipo a menos que haya sido capacitado para dar servicio tecnico. Siempre siga las instrucciones como se indican.</u>

1、Limpieza

Periodicamente la superficie del sensor óptico, el teclado y la pantalla necesitaran ser limpiados. Debido a que se trabaja en diferentes ambientes no se puede definir cuando exactamente se debe hacer limpieza. Siga esta guía:

Elemento	Frecuencia de limpieza
Teclado y pantalla	Limpie cuando la visibilidad se dificulte y se batalle para leer. Vea limpiar el teclado y pantalla descrito mas adelante.
Sensor Optico	No lo “sobrelimpie”. El sensor esta diseñado para trabajar en condiciones sucias o de poca grasa.
	De cualquier manera, límpielo, si el sensor se ve afectado o se reporta que la gente tiene dificultades para verificarse. Vea Limpieza del sensor optico.

２、Limpiando el teclado y la pantalla

Para limpiar el teclado y la pantalla use el mismo tipo de productos como los de ropa delicada y una toallita humeda.

３、Limpiando el Sensor Optico

Limpie el sensor óptico como se indica a continuacion:

(1) Si esta sucio o arenoso, primero sople sobre la superficie para elminar las particulas de polvo.

(2) Use cinta adhesiva para limpiar la superficie del sensor.

(3) Usando un trapo suave y seco. Tenga cuidado de no rayar la superficie del sensor. Si hay partículas de pelusa en la superficie del sensor, sóplelas cuando el sensor este seco.

Precaucion:

No utilize ningún otro limpiador de lo contrario el sensor podría ser dañado.

Limpiar con sustancias que contengan alcohol o alguna otra sustancia "fuerte" pueden descolorar o romper el gabinete del equipo.

Solucion de problemas

1. **Q: Las huellas de algunos usuarios a veces no pueden verificarse.**

A: Motivo: Puede ser porque el personal solo “golpetea” el sensor y no coloca bien el dedo. La calidad de la huella no es buena.

1) En algunos dedos la huella es muy tenue;

2) Las “ondas” de la huella son muchas o cambian por cortaduras o el tipo de trabajo;

3) La piel del dedo esta “cambiando”

Medida: Se le recomienda escoger un dedo “bueno” (que no se este “despellejando”, que tenga una imagen clara de la huella) cuando enrole una huella, procure que el dedo toque la mayor area posible del sensor, se le sugiere que enrole mas de una huella. Por cierto, nuestro equipo soporta método de coincidencia 1:1 e identificacion de contraseña, usted podrá escoger una de ellas.

2. **Q: Cual es la razón que el lector de huellas falle en la comunicacion?**

A: Las posibles razones:

1) La configuracion del Puerto de comunicaciones no esta correcta; el Puerto elegido para la comunicacion no es el Puerto que se esta utilizando.

2) La velocidad de comunicación entre el equipo y la computadora son diferentes.

3) El equipo lector de huellas esta mal conectado a la fuente de poder o a la computadora;

4) El lector de huellas esta conectado pero no se ha iniciado.

5) El numero de la terminal conectada no es el correcto.

6) La línea de datos o el convertidor falla en la comunicacion.

7) El puerto COM de la PC esta fallando.

3. Q: Despues de encender el equipo, la pandalla se muestra incompleta, solo la mitad o a veces desordenada; que pasa, como se puede solucionar?

A: La posible razón es:

1) La tarjeta principal esta dañada;

2) Problemas con la pantalla LCD. Tendra que contactar con su proveedor y mandarlo a reparacion.

4. Q: Como eliminar al administrador del equipo de asistencia？

A：**1)**.Puede utilizar el programa de asistencia del equipo en la computadora; en el software accede a la pagina de “administracion de equipo de asistencia”, clic en el boton de “Cancelar administrador” y podrá elminar al administrador, después de esto podrá entrar en el menú del equipo.

2). Llame al soporte tecnico de algun telefono cerca del equipo y asi lo podran ayudar a solucionar ese problema con el procedimiento necesario.

5. Q: Cuando conecta el equipo lector de huellas con un medio de comunicación el equipo hace un sonido “ding, ding”, cual es la

razón de ese sonido?

A: 1) Cuando se usa comunicación por RS-232, tal vez la velocidad de la computadora es diferente a la del equipo.

2) Si utiliza comunicación por RS-485, tal vez el convertidor este mal conectado.

6. **Q:Despues de encender el equipo, la pantalla siempre muestra el mensaje "Intente de Nuevo por favor"**

A: Causa: ① Despues de mucho tiempo de uso, la superficie del sensor se ensucia, o hay mucha pelusa sobre el, el equipo lo toma como si fuera una huella y realiza la verificacion

② El cable del sensor esta desconectado.

③ El chip de la tarjeta no funciona.

Medida: ① Puede utilizar un poco de cinta para limpiar la suciedad

② Necesita contactar al distribuidor para una reparacion

③ Necesita contactar al distribuidor para una reparacion.

7. **Q: Cuando se trabaja con el equipo, se descargan las huellas y las contraseñas correctamente, pero cuando se quieren leer para checar el registro de asistencia el sistema muestra que hay una falla, como se puede solucionar?**

A: Esta situación se puede dar por la línea de datos, algún convertidor, puerto COM de la PC, cuando esto ocurra puede reducir la velocidad de la computadora y del equipo lector de huellas, podría establecerlo como 19200 o 9,600, ahora intete hacer el proceso de nuevo.

Apendice

Las funciones descritas en el apéndice son adicionales, si necesita un equipo con alguna de estas funciones por favor consulte con nuestro encargado de ventas.

Administracion de USB

Definicion de USB

Un USB es el sustituto de los discos flexibles, es muy comun su utilizacion. Es muy pequeño, de gran capacidad de almacenamiento, de facil manejo y es un dispositivo “Plug and Play” de fácil uso.

Ventajas de usar un USB

1. La velocidad de transmicion es muy rapida, los lectores de huella “tradicionales” solo soportan comunicación por RS232, RS485 o Ethernet, lo que resulta una limitación física para transmitir mucha información y con esto el tiempo de transmicion también se eleva. Pero con la transmicion por USB es mas rápido que cualquier otro modo de transmicion, puede completar muy rápidamente el traspaso de información y mejorar la eficiencia.

2. Plug and play, de fácil uso. Cuando necesite descargar

información solo conecte el USB en el equipo para realizar la descarga, despues ponga el USB en la computadora para realizar la exportacion de datos. Ademas nuestro equipo lector de huellas también soporta pasar la información de usuarios y de huellas de un equipo a otro. Con esto se resuelve el trabajo tedioso de los lectores tradicionales y la computadora transmitiendo datos.

Como usar el USB para transmitir datos?

Los equipos lectores de huellas con el puerto de USB permiten usar estas memorias para descargar y subir información. Acerca de la administración de USB vea el capitulo 6 de este manual.

Teclas condicionales

En el equipo de Time&Attendance para cada evento corresponde una condicion, por ejemplo de acuerdo a la situación el estado de trabajo puede dividirse en: checar entrada (clock in), checar salida (clock out), checar entrada de tiempo extra (overtime check-in), checar salida de tiempo extra (overtime check out), salida y regreso (going out, return in), el equipo de control de acceso divide en “entradas” y “salidas” las diferentes situaciones:
En algunos equipos los teclados tienen 6 teclas condicionales para establecer la condición actual. Puede presionar "▲" y "▼" para seleccionar la condición actual. Pero estas opciones necesitan ser cambiadas manualmente, las condiciones se utilizan de acuerdo al correspondiente estado del boton. Para reducir la operación manual

podemos hacer una programación especial para realizar estos cambios, asi cuando se llegue el tiempo que el usuario establezca el equipo podra cambiar la condicion actual automaticamente y mostrarla en la pantalla inicial. Si necesita un equipo con esta modificación por favor contacte con nuestro encargado de ventas, para mas detalles vea el punto 5.2.2

Tiempo de campana

En algunas empresas se utuliza una “campana” para mandar un mensaje a los empleados cuando empiezan o terminan sus labores, la manera tradicional es activar una campana manualmente o por un equipo electronico en especial, nosotros pusimos una campana en nuestro equipo T& A, usted se beneficiara a un bajo costo y tendrá una mejor administracion. Hay mas de dos opciones para programar la campana y su duración en el equipo que cuente con esta opcion. En total el sistema tiene un total de ocho programaciones a establecer, de acuerdo a su necesidad puede configurar la hora de la campana, cuando se llegue la hora programada el equipo automaticamente hara sonar la campana, la campana dejara de sonar automaticamente.

Hay dos maneras de hacer sonar la campana:

1. Mandar un sonido desde la bocina del equipo.

2. Conectar una campana al equipo, cuando se llegue la hora el equipo enviara una señal para activarla.

Para mas detalles vea (introducción al tiempo de timbre).

Sensor externo de huellas

Esta es una funcion exclusiva de los equipos con puerto USB, conecte el sensor de huellas en el Puerto USB, entre a menu->Opciones->Opciones avanzadas->Sensor de huellas externo y establezca la opción “Sensor externo” como “Y”. Ahora el sensor externo y el interno se encuentran en el equipo y pueden ser usados juntos.

En aplicaciones de T&A esto ayuda al sistema ya que hace que el proceso de cuando checan todos los empleados su entrada o salida sea mas rapido.

Para aplicaciones de Control de Accesos el lector externo puede estar ubicado en la parte de afuera de una puerta y el equipo principal en el interior, esto podria ayudar a mejorar la seguridad del equipo principal.

Nota:

1) Despues de conectar el sensor externo asegurese de reiniciar el equipo para que los cambios tengan efecto.

2) El sensor externo no puede ser utilizado hasta que se establezcan los permisos en el SDK.

Funcion de modem

Para lograr que la PC y el lector de huellas se comuniquen remotamente sin una red local, algunos tipos de equipos soportan la conexion PPP, la conexion PPP en una conexion punto a punto a traves de una linea, la PC no marca ni se conecta a una red a traves del modem hasta que el lector de huellas se conecte con el modem y el telefono, luego marque y se logre exitosamente la conexion a la red.

Aviso de Modem:

1) Use el cable marcado como “Modem Cable” para conectar el modem con el equipo A11.(Nosotros proporcinamos el cable).

2) Debera usar el controlador del A11 para proveer energia al modem.

3) Antes de conectar el modem establezca el valor de “Modem Externo” como “Y” (**Menu-**> **Opciones-**>**Opciones de comunicacion-**>**Modem externo**) en el menú del A11.

4) Cuando se usa un Modem, RS232, RS485 para el A11 estan inhabilitados. Una vez que se establece como “N” el valor de “Modem Externo” (sin uso de Modem), RS232, RS485 vuelven a habilitarse.

5) Un servidor PPP ha sido agregado dentro del A11, utilice el programa

"Dial up" de windows que soporte PPP para conectarse con el A11, el usuario por defecto es ppp, al igual que su contraseña. Despues de establecer la comunicacion PPP, la direccion IP por defecto es 192.168.1.133, la dirección IP de la terminal de usuario sera 192.168.1.100.

6) Usando una conezion estándar de modem

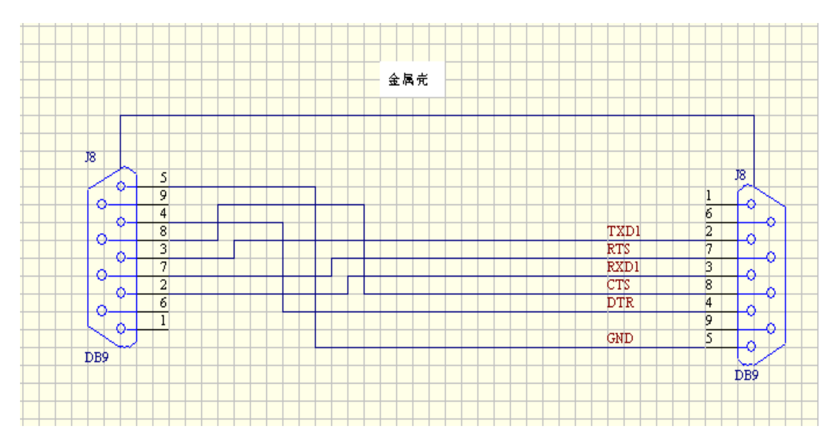


Figure: Modem Cable

Funcion de busqueda

Hay equipos lectores de huellas que soportan la funcion de realizar consultas para ver los registros de asistencia personal o de todos los empleados. Esto proporciona una solución a los problemas de que

el usuario tiene que esperar a que el software sea instalado, se conecte al equipo y descargue los registros de asistencia. La funcion de consulta provee al personal la funcion de conocer los registros de asistencia ellos mismos.

Este equipo no solo provee la opción de ver el registro de asistencia de una persona, puede hacer una consulta de todo el personal.

Para mayor información vea el capitulo 9, Ver registros de T&A.

Funcion de impresion

Esta funcion solo soporta impresoras conectadas por puerto (RS232), la interface del Puerto paralelo no es soportada, para imprimir puede conectarse directamente a la impresora y también puede conectarse con la PC para ver el contenido exportado.

Esta funcion soporta dos opciones: 1.impresion inmediata 2.ver el contenido exportado mientras se va a imprimir.

1. Impresion inmediata

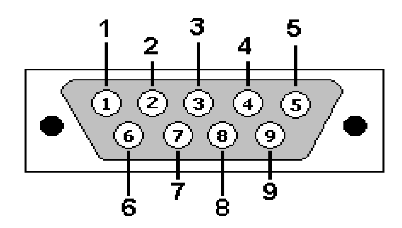
Entre a Menu-> Opciones->Opciones de sistema ->Opciones avanzadas->Impresion inmediata, establezca el valor como RS232 guarde los cambios y salga. El equipo imprimirá el registro después de cada verificacion.

2. Ver el contenido mientras se va a imprimir

Mientras se ven los registros desde el equipo lector de huellas,

presione (OK), el contenido que se muestra en la pantalla sera mandado a imprimir, el contenido exportado también será posible verlo en el “super terminal”.

El cable de conexión entre el equipo lector de huellas y la impresora:



Equipo lector de huellas   Impresora

2 TXD   <----->   3 RXD

3 RXD   <-----> 2 TXD

5 GND   <-----> 7 FG

Nota: la velocidad de transmicion del equipo lector de huellas y la impresora es la misma.

Administracion de mensajes cortos (Opcional)

Algunos de nuestros productos proveen la funcionalidad de mandar mensajes a personas asignadas a traves de la forma publica o personal, Solo necesitamos utilizar el software back-end para

establecerlo, despues subirlo al equipo lector de huellas, tan pronto se encienda el equipo el mensaje publico sera mostrado en la pantalla del equipo, éste se mostrara siempre, los mensajes cortos personales no se mostraran hasta que la verificación del usuario sea positiva, De este modo se reduce la carga de trabajo del administrador de recuersos humanos y mejora la eficiencia de trabajo.

Mande un mensaje al personal asignado, si el cumpleaños de una persona es el 20 de Octubre, podremos usar el software “back-end” para enviarle un mensaje corto como “Feliz cumpleaños”, súbalo en el equipo, después de que esa persona se verifique en ese dia el mensaje aparecerá en la pantalla del equipo.

Mande un mensaje publico, si la compañía necesita tener una junta el 19 de Junio, despues de que configuramos el “back-end” para subirlo al equipo, hasta este dia, el mensaje "reunion XX en la sala XX” aparecerá continuamente en la pantalla y les preguntara sobre XX participacion (desde luego puede revisar esa información de acuerdo a su necesidad).

Configuracion de la funcion de mensajes cortos: despues de establecer los mensajes cortos en el software de Time&Attendance y subirlos al equipo, el equipo soporta dos maneras de importar los mensajes cortos, una es que el software se conecte con el equipo para importarlos directamente, otra forma es por medio de USB.

El procedimiento es el siguiente:

1. A través del programa Time&Attendance “programa externo”—“administración de mensajes cortos” complete la configuración de mensaje corto, luego conéctelo al lector de huellas y suba la informacion, 2. A través del programa Time&Attendance “programa externo”—“administracion de mensajes cortos” complete la configuracion de mensaje corto, seleccione “programa externo”—“administracion de USB”—“exportar mensaje corto”—“exportar a USB”, después de terminar la exportación, conecte el USB al equipo lector de huellas, presione la tecla “Menu” vaya a —“Administracion de USB”—“Subir mensaje corto (SMS)”.

Efecto de la funcion de mensaje corto: Para mensajes cortos publicos seran vistos y se mostraran siempre despues de la verificacion exitosa del personal, el mensaje se mostrara en la pantalla.

Nota: Puede haber un total de 1024 mensajes entre publicos o privados.

Modo de autenticación Multi-combinacion

Esta funcion es incluida en el equipo lector de huellas con control de acceso; la mayoria de los lectores de huellas solo tienen dos maneras de verificar, por huella y por contraseña; proveemos un

modo de autenticacion de multi-combinacion personal o de grupo para tener mayor seguridad en el area de control de acceso, la verificación tiene cuatro elementos principales que son Numero PIN, Huella (FP), Contraseña (PW) y tarjeta RF (RF) y las puede combinar para crear una multi-combinacion.

Nota:

El equipo lector de huellas con funcion Mifare se necesita para la verificacion con tarjetas Mifare.

La tarjeta Mifare se considera como una tarjeta RF en el proceso de verificacion, la funcion de verificacion por tarjetas Mifare solo es valida en los equipos que tengan provista la opcion de tarjetas Mifare.

A continuación se define lo que significan los simbolos de la tabla de abajo.

● "/" es "or", ● "←" es confirmar (Enter),

●"+" sigue a la siguiente operacion ● "&" es "and",

● FP (huella) ● PWD (Contraseña)

● RF (tarjeta RF) ● PIN (ID de usuario)

Si la huella o contraseña se han usado para enrolar un usuario, el procedimiento de verificación es el siguiente:

Tipo	Lo que hace
FP	Solo la huella es verificada. 1） PIN+FP（Verificacion 1：1） 2） FP (Identificacion 1：N) 3）RF+FP(1:1)
PIN	Solo el PIN es verificado 1）PIN(introduzca los digitos con el teclado)
PW	Solo verificación de contraseña es verificada 1） PIN+“←”+PW 2） RF+PW
RF	Solo tarjeta RF es verificada 1）RF
FP/PW	Huella o contraseña se verifican 1） PIN+FP(1:1) 2）FP(1:N) 3）PIN+“←”+PW

	4）RF+PW
FP/RF	Huella o RF se verifican 1）PIN+FP(1:1) 2）FP(1:N) 3）RF
PW/RF	Contraseña o RF se verifican 1） RF 2） PIN+“←”+PW
FP/PW/RF	Huella o RF o Contraseña se verifican 1） PIN+FP(1:1) 2） FP(1:N) 3） PIN+PW 4） RF
FP&PIN	Huella y PIN son verificados 1）PIN+“←”+FP(1:1) 2） RF+ PIN+“←”+FP(1:1)
FP&PW	Huella y PIN son verificados

	1）FP(1:N)+PW 2）PIN+FP(1:1)+PW 3）RF+PW + FP(1:1)
FP&RF	Huella y RF se verifican 1）RF+FP(1:1) 2）FP(1:N)+RF 3）PIN+FP(1:1)+RF
PW&RF	Contraseña y RF se verifican 1）RF+PW 2）PIN+“←”+PW+RF
FP&PW&RF	Huella, contraseña y RF se verifican 1）FP(1:N)+PW+RF 2）PIN+FP(1:1)+PW+RF 3）RF+ PW+ FP(1:1)
FP&PIN&PW	Huella, PIN y contraseña se verifican 1）PIN+“←”+PW+FP(1:1) 2）RF+ PIN+“←”+PW+FP(1:1)
FP & PIN /RF	Huella y PIN, o RF se verifican

	1) FP+ PIN 2) FP +RF 3) PIN+FP(1:1) + PIN 4) PIN+FP(1:1) +RF

Nota:

1) Autenticacion 1: N incluye la autenticacion 1: H, 1: G.

2) En la autenticación multi-combinacion, es mejor utilizar huella y contraseña para enrolar, de otra forma, algunas veces fallara la verificacion.

Soporte de tarjetas(HID, iCLASS, EM, Mifare)

Con el fin de satisfacer las necesidades del mercado de seguridad, nuestros biométricos lectores de huellas tienen integrados módulos de lectura de HID, iCLASS, EM, Mifare**.**

Los módulos HID iCLASS 50 OEM, EM y Mifare pueden ser usados para actualizar la verificación biométrica de huellas para aumentar el nivel de seguridad.

Usando la tecnología inteligente "sin-contacto" 125MHZ, 13.56 MHz, estos productos proveen a los usuarios nuevas opciones de soporte de multi-autenticacion de identidad. Combina una presentación de tarjeta "sin-contacto" con un biométrico de huellas digitales. O, use un número de identificación personal (PIN) junto con la presentación de tarjeta "sin-contacto". (Vea multi-autenticacion).

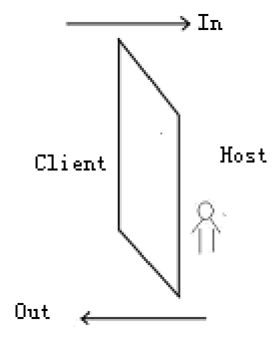
Los equipos lectores de huella proveen tres niveles de verificación de huella. Durante el proceso de enrolado, la pantalla guiara al usuario para poner su dedo en el sensor. La plantilla de la huella es recogida por la unidad e inmediatamente se transfiere a la tarjeta. Durante este proceso de enrolado, la plantilla de huella es almacenada en la tarjeta y en el equipo.

Durante la verificación en la puerta, la pantalla asistirá al usuario con las instrucciones para colocar el dedo en el sensor biométrico.

Para más detalles vea “Guía de uso de tarjetas HID, iCLASS, EM”

Acerca de lectores de huellas Cliente-Servidor

Resumen



Hay dos equipos lectores de huella para controlar una cerradura juntos, un equipo es nombrado como cliente (client) en la parte de afuera, otro es definido como servidor (host) adentro y estos ofrecen la mejor solución de conexión con dos equipos que controlan una puerta.

El propósito de la información del usuario, identificación de huella y validación de privilegios se encuentran el “servidor”, el equipo cliente solo es usado como lector de huellas, el programa solo administra la información de usuario y registros de asistencia del equipo servidor. Esto ayuda ya que toda la información se encuentra en un equipo y reduce los problemas de administración.

Este sistema también le provee la función de anti-passback, previene que un usuario no autorizado entre ya que no podrá abrir la puerta para salir. Esto significa que si un usuario no registra su entrada, entonces ocurrirá una violación al Anti-passback y no podrá salir.

Empezar el trabajo

Equipo servidor: Enrole y verifique las huellas, configure los privilegios de usuarios, valide los privilegios de usuario, recibir información de tarjetas y huellas del equipo cliente, verificarlas y mandar los resultados de Nuevo al equipo cliente.

Equipo cliente: Solo se usa como lector, su trabajo es recolectar las huellas, leer tarjetas y mandar la información que necesita ser verificada en el equipo servidor, el servidor es el que mostrara los resultados de la validación.

Instrucciones de la característica cliente-servidor

1) Guardar logs

Por defecto el estado del equipo servidor como salida, el estado del equipo cliente como entrada y todos los logs se almacenan en el equipo servidor.

2)Funcion Anti-pass back

Dependiendo del tiempo de entrada y salida se determina si ocurre una violación de anti-pass back, el registro de entrada y salida están asociados, Este equipo soporta tres tipos de anti-pass-back, son

salida, entrada, entrada y salida (entre a menú –>opciones->sistema->opciones avanzadas –> anti pass back), ahora escoja “out anti-pass back” como ejemplo.

Si alguien desea salir.

1) El/Ella no tiene checada la entrada, el sistema mostrara “Anti-pass back rejects”, rechaza la apertura de la puerta.

2) El/Ella si checa la entrada, el sistema lograra la verificación y abrirá la puerta.

“In anti-pass back” y “Out anti-pass back” son de logica similar

Aviso：Asegúrese de reiniciar el equipo para que los cambios tengan efecto.

3) Función de alarma

Si la alarma que viene integrada en el equipo lector de huellas (como un F10), cuando ocurra un evento de alarma en el equipo cliente, la señal de alarma será enviada al equipo servidor para ser procesada. Si el equipo no cuenta con la función de alarma esta característica será invalida.

Como usar equipos cliente y servidor

1) Seleccione el modelo del equipo

Servidor：Comúnmente se utilizan equipos que tienen la habilidad

de abrir puertas como los ZEM 100 series: F7. F4. A3 etc.

Cliente：Podrá seleccionar cualquier equipo lector de huellas de la serie ZEM 100 que cumplan con la condición de comunicación RS232

Nota ：Solo las versiones de firmware arriba de la 5.22 pueden soportar la función de cliente servidor.

2) Configurar el menú del servidor

Entre a "Menú - Opciones - Opciones de sistema – Opciones avanzadas"，aquí hay tres opciones:

Cliente y servidor：Este equipo puede definirse como servidor por la opción de "Servidor", "Cliente" o "No" (después de configurar asegúrese de reiniciar el equipo para que esta opción tenga efecto)

Mostrar la operación del cliente：Si se define como "Yes", la operación del cliente será mostrada en el servidor, de otra forma la operación del cliente no se mostrara (esta opción no se muestra hasta que el cliente lo define como servidor)

Anti- pass back：Esta opción puede definirse como “Out anti-pass back”, “In anti-pass back”, “In-out anti- pass back” and “No” (esta opción no tendrá efecto hasta que reinicie el equipo)

3) Conectar el servidor con el cliente

4) Después de seleccionar el equipo, conecte el servidor con el cliente por RS232, la conexión de cables seria:

Servidor		Cliente
TXD	<----->	RXD
RXD	<----->	TXD
GND	<----->	GND

Nota：Ahora el cliente y el servidor solo podrán soportar RS232.

Es diferente de una conexión con una PC, las conexiones RX y TX se intercambian, la conexión GND se conecta directamente una con la otra.

b) Realice la conexión antes de prender el equipo, el equipo cliente “corre” como un equipo normal de control de acceso y puede buscar al cliente automáticamente mientras se enciende.

Si el mensaje “conn. mst failed” se muestra en el equipo cliente, significa que falló la conexión con el servidor, probablemente falle la comunicación, la bocina sonara tres veces, por favor revise la comunicación del cliente y el servidor.

Si el mensaje “mst unsupport” aparece en el equipo cliente significa que no soporta la función de servidor, la bocina sonara tres veces, por favor revise la configuración para ver si esta correcta.

Si no hay información mala en el cliente y el servidor, muestra que la conexión del cliente y servidor ha sido exitosa y puede ser usada, tome el servidor como un equipo normal de control de acceso, el cliente realiza la siguiente tarea: recolectar huellas, examinar y enviar el contenido de entrada del usuario y mostrar el resultado del equipo servidor. El servidor implementa la operación de coincidencia de huella 1:N, 1:1, verificación de contraseña, validez de tarjeta ID.

Solución servidor remoto

Debido a la capacidad y velocidad del equipo independiente, resulta imposible agregar muchos equipos lectores de huella (por ejemplo, 10 mil lectores). Aunque la capacidad sea expandida, la velocidad del equipo independiente se verá afectada; la velocidad es mucho más baja que la de una PC. Basado en estas razones el equipo independiente es incapaz de trabajar en esos grandes sistemas que tienen la capacidad de muchas huellas y alta eficiencia de coincidencia, así que la solución sería utilizar un servidor remoto el cual pueda tener gran capacidad y una eficiencia alta.

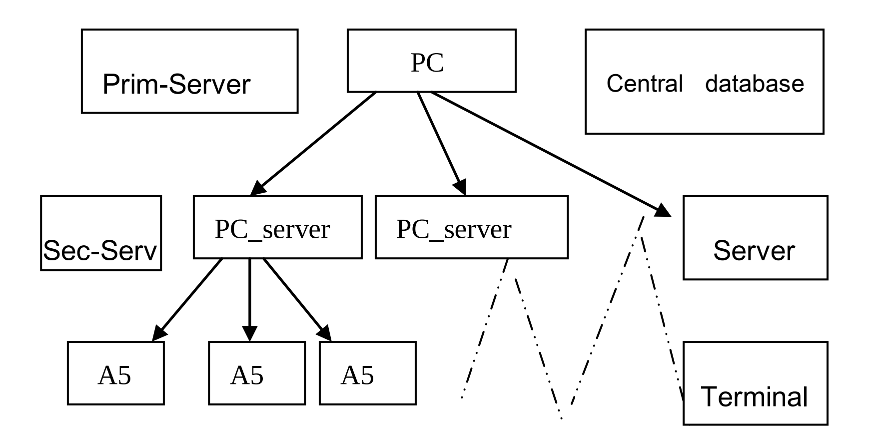
Concepto

Tomando el equipo independiente como un escáner de huellas, se reserva su función de identificación independiente. Con la identificación y verificación, se almacenan los resultados de coincidencia en una BD (Base de datos) oculta y se muestran los resultados en la pantalla del lector de huellas para completar la tarea del proceso de identificación. Si el algoritmo de identificación adopta la propiedad intelectual del algoritmo BioKey, entonces las PC comunes pueden actuar como un servidor remoto, la solución de servidor remoto tiene menos requerimientos de todo el sistema de identificación y mejora el algoritmo de eficiencia, por lo tanto se asegura la viabilidad y conveniencia de esta solución.

Propósito de solución: para gran capacidad de identificación de huella, mayor administración interna de la empresa, administración inteligente, control de Entrada/Salida del personal.

Arquitectura de un servidor remoto

Para adoptar el modo básico de C/S siga la siguiente figura:



Asigne en un servidor primario una partición para actuar como base de datos central. En algunas aplicaciones, puede seleccionarse un servidor especial para asegurar que cada servidor secundario puede accesar fluidamente a la base de datos, el servidor primario también puede actuar como servidor remoto, y es en el servidor secundario con respecto al rol del servicio de identificación e idéntico con otro servidor remoto. La única diferencia entre ellos es que el servidor primario puede jugar dos roles, por ejemplo, servicio de base de datos + servicio de identificación. En la actualidad, el servicio de base de datos en mediante SQL Server.

Como lo muestra la figura de arriba hay tres niveles y están divididos lógicamente. La dirección del flujo de datos de identificación es:

Servidor primario:

1. Escaneo de huellas.

2. Resultados de identificación exitosa.
3. Configuración inicial de la aplicación del sistema.

Servidor secundario:

1. Datos de huellas del servidor primario.
2. Información de coincidencia de huella pasado por el servidor de nivel tres.

Servidor de nivel tres

1. La información de huella se obtendrá en el momento de que se pongan las huellas.
2. Entrada de teclado.

Para más detalles por favor contacte con nuestro servicio técnico.

iClock Time & Attendance

Resumen de IClock

iClock es basado en "Web Server" sistema técnico Time&Attendance. Solicitud técnica para procesar y administrar información, integra muchas funciones, como recolección local de datos, puertos (RS232/RS485), conversión de protocolo de comunicación, recolección de imágenes, datos de alarmas almacenadas, WEB server etc. Basándose en este equipo para crear una plataforma unificada de monitoreo que proporcione una solución para la administración de equipos, Time &Attendance,

como monitor, en conjunto con la solución Web Time & Attendance es independiente del límite regional y no necesita instalar software adicional. Utilice su navegador IE o Netscape, descarga y administración remota en línea, está disponible el manejo de corrección de tiempos y crear tablas de reportes en la terminal de huellas, provee una fácil manera para que el gerente de empresa conozca el estado de asistencia en cualquier momento, búsqueda de información, datos estadísticos, tratar con la operación al mismo tiempo, proveer una solución para la asistencia de empleados, administración de entradas o salidas, administración de roles de pago, de palabra y de hecho darse cuenta que en todas partes a cualquier momento la información esta sincronizada, esto va mas allá de la solución tradicional de Time&Attendance.

Porque incorporar un servidor web en un equipo lector de huellas

1. Unos pocos o nadie vigila

A través de TCP/IP y Ethernet, servidor web se puede aplicar a la red local, los datos almacenados en el lector de huellas pueden ser vistos desde una gran distancia, con el navegador no es necesario tener una persona para que vaya físicamente a recolectar datos, subir y bajar información, así como actualizar el sistema, no necesita de otros software o herramientas

2. Completamente compatible con el programa de nuestra empresa. La plataforma de WEB Server puede ser completamente compatible con el programa actual asi el beneficio es mutuo, la habilidad de ser más flexible para las necesidades del cliente.

3. Más fiable, rápida transferencia de datos a través de largas distancias

A través de WEBSERVER, es fiable y rápida la descarga de los datos al sistema local, utilice la capacidad de descargar todos los datos en poco tiempo, no se preocupe por la fiabilidad de los datos

4. Más flexibilidad, facilidad de administración de los datos

A través de la plataforma creada por el Web server, el programa, la administración de datos se vuelve más fácil y flexible.

5. Puede ser fácil integrar sistemas OA, CRM, base fiable en la gestión del personal.

Como usar equipos lectores de huella de la serie iClock

Esta serie de equipos tiene soporte para tres tipos de conexiones—LAN, Dial –Up telephone, internet a través del Web server, primero inicie sesión en el sitio de bioiclock, identifique su equipo, por defecto el nombre y contraseña es administrador y nuestra compañía.

Nota: Para más detalles vea la guía de Usuario iClock

Control de acceso servidor Web

Resumen de control de acceso con Web Server

Anunciamos la salida de la nueva versión de control de acceso, la nueva versión se basa en la técnica de Web Server y en la arquitectura TCP/IP, utilice la pagina WEB para procesar y administrar datos, además la solución del control de acceso con Web Sever es independiente de los limites regionales, permite descargas y administración remota en línea del equipo lector de huellas a través de IE o Netscape, manejar correcciones de tiempo y crear tablas de reporte, esto va mas allá del software tradicional de control de accesos, también se incorpora la experiencia de muchos años del equipo.

La función del Web Server integrado

Por favor vea iClock Time & Attendance》。

Guía de usuario de Webserver.

Si es la primera vez que utiliza el software de WebSever, introduzca la dirección IP del equipo lector de huellas, Ej., la dirección IP del lector de huellas es 192.168.1.115, introduzca http://192.168.1.115 en la barra de direcciones de IE, por defecto el súper administrador del sistema es admin, la contraseña es admin 888. Para detalles del software WebServer por favor vea (Websever Access Control Explain)

Obtener dirección IP automaticamente

Tal vez las siguientes circunstancias pueden ocurrir, si hay muchos equipos lectores de huellas en la red corporativa, el administrador tal vez olvido la dirección IP del equipo lector de huellas, los administradores pueden checar la dirección IP en el sistema pero es una difícil tarea, especialmente cuando múltiples sistemas están involucrados y existe mucho margen de error, nosotros desarrollamos un software para detectar la dirección IP de los equipos lectores de huellas en la red local.

Copie todos los archivos DLL en la carpeta system32 del directorio del sistema, click en inicio->ejecutar->regsvr32 zkemkeeper.dll, el sistema mostrara el registro exitoso, doble click en Machine Search.exe para ejecutar el programa.

Acerca de Wiegand

Wiegand es una interfaz comúnmente usada entre lectores y paneles de control usados en el control de acceso, seguridad, asistencias y otras industrias. Software de los equipos de control de acceso serie F se basan en el estándar Wiegand especificado por el protocolo estándar de control de acceso de la Asociación de la Industria de Seguridad (SIA) en el documento “26-Bit Wiegand Reader Interface”. Los fabricantes han adoptado el estándar Wiegand para establecer una interface en común. Esto provee un

nivel de compatibilidad e interoperabilidad para lectores y paneles de control que pueden ser utilizados por consultores, especificadores y los usuarios finales a la hora de establecer el diseño del producto o los criterios de la instalación del sistema.

Señales de datos

La figura 1 muestra el patrón de tiempo de los bits de datos enviados por el lector al panel de control de acceso. Este patrón de tiempo se encuentra dentro de la guía Wiegand como se describe en el protocolo de control de acceso de la SIA para el documento "26-Bit Wiegand Reader Interface" (el tiempo del ancho de pulso entre 20 µS y 100 µS, y un tiempo de intervalo de pulso entre 200 µS y 20 mS). Las señales Data 1 y Data 0 se mantienen en la logica de alto nivel (por encima del nivel Voh) hasta que el lector está listo para enviar el flujo de datos. El lector coloca los datos como pulsos de bajo curso asíncronos (abajo del nivel Vol) en las líneas Data 1 o Data 0 para transmitir el flujo de datos al panel de control de accesos (las "ondas" de la figura 1). Los pulsos Data 1 y Data 0 no ocurriran simultaneamente. La tabla 1 provee el mínimo y máximo tiempo de ancho de pulso permitido (la duración del pulso) y los tiempos de intervalo de pulso (el tiempo entre pulsos).

Tabla1 Pulso

Símbolo	Descripción	Tiempo típico del lector
Tpw	Tiempo de ancho de pulso	100µm
Tpi	Tiempo de intervalo de pulso	1ms

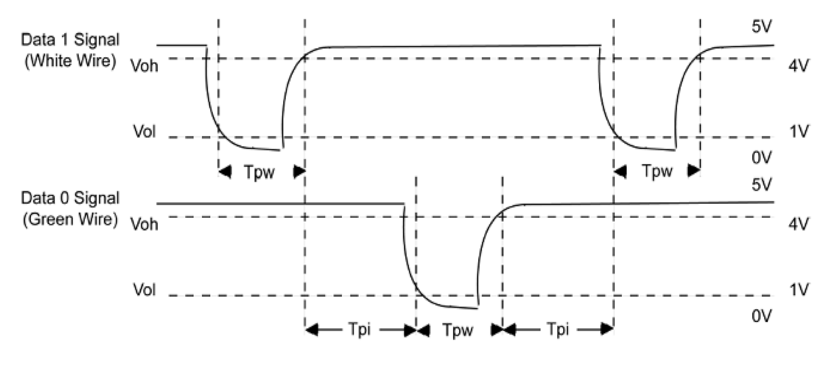


Figura 1 Tiempo

Formato Wiegand

El formato de Wiegand de los controles de acceso serie F es un protocolo general de control de acceso.

Formatos 26-bit Wiegand

La composición del estándar 26 Bit Wiegand contiene 8 bits para la instalación del campo de código y 16 bits para el campo de numero ID. Matemáticamente estos 8 bits de instalación de código permiten un total de 256 códigos de instalación (0 a 255), mientras que los 16 bits del numero ID permiten un total de solo 65,536 (0 a 65,535) ID individuales en cada código de instalación.

La longitud de 26-Bit Wiegand es de 26 Bit, esto incluye dos bits de paridad.

1	2 9	10 25	26
EP	**FC**	**CC**	**OP**

Table field definition

Campo	Propósito
EP	Bit de paridad Even, de los bits 1 a 13, si hay Even “1”, EP es 0; oposición sera 1.
FC(bit2-bit 9)	Código de instalación (0-255), Bit 2 es MSB (bit más significativo)
CC (bit10-bit 25)	Código de tarjeta,(0-65,535) , bit10 es MSB (bit más significativo)
OP	Bit de paridad Odd, OP se define por encima del bit 13 al 26, si hay odd “1”, oposición será 0

Formato de la pirámide Wiegand

Existen muchas alternativas para los clientes que requieren más códigos. La primera es cambiar al estándar de Keri, el formato de pirámide 39 bit. Este formato 39 bit Wiegand contiene 17 bits para el código de instalación y 20 bits para el campo de numero de ID. Matemáticamente estos 17 códigos de instalación permiten un total de 131,072 (0 a 131,071) códigos de instalación, mientras que los 20 bits del numero de ID permiten un total de 1,048,576 (0 a 1,048,575) ID individuales dentro de cada código de instalación. Ya que hay tantos códigos de instalación en el formato de pirámide, un nuevo código de instalación puede ser seleccionado para cada

proyecto. Adicionalmente, el largo numero de ID por código de instalación hace al formato de pirámide ideal para proyectos muy grandes. Para mayor seguridad, codificación de pistas de credencial Keri Systems aseguran que no ocurra una duplicación.

Table-3 Formato de pirámide Wiegand

Numero de Bit	Propósito
Bit 1	Even parity sobre bits 2 al 19
Bits 2 a 18	Código de instalación (0 al 131,071); Bit 2 es MSB
Bits 19 a 38	Numero ID (0 a 1,048,575); Bit 19 es MSB
Bit 39	Paridad Odd sobre bits 20 al 38

Formatos Wiegand personalizados

La segunda alternativa es crear un formato Wiegand personalizado. Típicamente, hay disponibles hasta 64 bits para crear un formato Wiegand personalizado. Con ciertas limitaciones, formatos con más de 64 bits pueden ser creados. Si el cliente actualmente tiene un formato Wiegand personalizado de Wiegand o de otros fabricantes similares, Keri normalmente puede coincidir con ese formato. Aunque el cliente es primeramente responsable de la codificación de tarjeta personalizada, como un beneficio extra se incluye “Keri Systems tracks card coding” para mayor seguridad.

Table-4 Ejemplo de un Formato Wiegand Personalizado

Numero de Bit	Propósito
Bit 1	Paridad Even del bit 2 al 22
Bits 2 a 9	Código OEM (0 a 255); Bit 2 es MSB
Bits10 a 21	Código de instalación(0 a 4,096); Bit 10 es MSB
Bits 22 a 43	Numero ID (0 a 524,287); Bit 22 es MSB
Bit 44	Paridad Odd del bit 23 al 43

Entendiendo SOAP

Definicion de SOAP

SOAP es un protocolo ligero destinado al intercambio de información estructurada en un descentralizado, distribuido ambiente. SOAP utiliza tecnología XML para definir un marco extensible de mensajería, que provee un constructor de mensaje que puede ser intercambiado sobre una variedad de protocolos subyacentes. El marco ha sido diseñado para ser independiente de cualquier modelo de programación en particular y otras especificaciones de implementación.

Aplicación SOAP

Nuestro equipo lector de huellas puede soportar completamente XML-based soap, puede construir requerimientos de su software en SOAP, utilícelo para descargar o subir información de usuarios,

información de huellas y registros de verificación. Es conveniente importar estos datos a la base de datos de la empresa, también puede satisfacer la administración de empleados de la empresa y diferentes solicitudes de software.

Nota：Si desea más detalles contacte a nuestro asistente técnico.

Acerca de POE（Power over Ethernet）

Resumen

Power over Ethernet (PoE) es una tecnología revolucionaria que extiende la actual amplia funcionalidad del Ethernet agregando un suministro fiable de fuente de poder sobre el mismo cable de par trenzado categoría 5/5e que actualmente lleva los datos de Ethernet. PoE, es el modelo de la tecnología usada por las industrias de telecomunicaciones para proveer energía fiable a teléfonos, permite la calidad de energía para teléfonos IP (VoIP) así como de otros equipos de red Ethernet como wireless access points (WAP) y cámaras de seguridad.

Aplicación de POE

Después de poner el equipo lector de huellas con PoE integrado dentro de un sistema PoE, no es necesario poner el adaptador para proporcionar energía, su trabajo normal solo depende del suministro PoE, esta forma provee un bajo costo y mayor flexibilidad de instalación, la tabla 1 muestra el numero de pin del conector Ethernet RJ45 del equipo lector de huellas.

Tabla 1 Número de pin del conector RJ-45 (De izquierda a derecha)

Numero	Color de cable	Fuente
1	Blanco/Naranja	TX+
2	Naranja	TX-
3	Blanco/Verde	RX+
4	Azul	Power
5	Blanco/Azul	Power
6	Verde	RX-
7	Blanco/Café	GND
8	Café	GND

Beneficios de POE

Bajo costo. PoE elimina la necesidad de poner ambos cables, los de datos y energía a cada dispositivo en la red. WAPs y cámaras de seguridad pueden ser instaladas sin el costo extra de contratar un eléctrico para instalar los contactos de AC donde se desean. PoE también ayuda a proteger las inversiones de IT ya que es compatible con otros protocolos ethernet. Además, equipos PoE

que son manejables por Simple Network Management Protocol (SNMP) pueden ser monitoreados y controlados remotamente para un manejo eficiente o resolución de problemas de consumo de energía y/o fallas.

• *Mayor flexibilidad*. Equipos de la red pueden ser instalados y reubicados donde su rendimiento sea optimo y no estén atados a un contacto existente de AC. Esto es especialmente importante para equipos como WAPs, que pueden ser instalados en lugares difíciles de alcanzar como el techo para poder alcanzar la mejor cobertura.

• *Mas fiable*. Una SNMP manejable fuente de energía centralizada mejora la protección contra sobrecargas o cortes de energía. Cuando se implementa PoE, a lo largo de una fuente de energía ininterrumpida (UPS) o respaldos de baterías, permite a las empresas distribuir energía aunque se interrumpa el suministro de corriente eléctrica. Esto les permite reemplazar los teléfonos convencionales con teléfonos VoIP conservando al mismo tiempo los beneficios de fiabilidad.

Batería de reserva (Mini-UPS)

Es importante asegurar el suministro de energía para el lector de huellas bajo cualquier circunstancia, por lo tanto además del adaptador estándar que proveemos, también contamos con el Mini-UPS especial de 5V, de acuerdo a su actual necesidad de comprarlo, de acuerdo a su posibilidad, ayuda a aliviar el problema de la administración de energía que podría hacer que el lector de

huellas se apague.

Principio del trabajo

En estado normal, la batería de reserva se encuentra en estado inactivo, el lector de huellas se provee de corriente directa que es suministrada por un adaptador de corriente, si la bacteria de reserva esta en el estado de "non-saturation", se cargara automáticamente. Cuando se corte la energía, la batería de reserva cambiara al estado de "discharge" para alimentar al equipo lector de huellas.

Como seleccionar la batería de reserva

modelo	Duración
ZK-B1 (2000mAh)	3 horas
ZK-B1 (4000mAh)	6 horas

Modo de conexión



Nota：Por favor asegúrese de conectar primeramente el Mini-UPS al lector de huellas y luego encenderlo.

Almacenamiento de baterías

Cuando se almacenan las baterías, SIEMPRE almacénelas en un lugar fresco y seco de una temperatura de (-10℃～30℃). NO almacene las baterías bajo los rayos directos del sol, temperaturas altas o humedad alta, por mas de 3 meses de almacenamiento es necesario mantener la capacidad de carga en un 50% (cargue las baterías al menos una vez cada tres meses), mantenga las baterías lejos del alcance de sustancias químicas y alejada del fuego o lugares muy calientes.

Aviso

Existe peligro de explosión de la batería, fugas, sobrecalentamiento, fuego o ruptura si no lee el aviso con cuidado.

- NO ponga la batería en agua o permita que se moje.
- NO utilice o almacene la batería en lugares cerca de equipos que generen calor (como fuego o calentadores);
- Por favor utilice solo el cargador original;
- NO invierta la polaridad de conexión;
- NO conecte las baterías directamente en la salida de corriente o en el cargador de carro sin antes poner el cargador entre las baterías y la fuente de energía;
- NO tire las baterías al fuego.
- NO utilice cable u otro material para conectar el polo negativo con el positivo de la terminal
- NO rompa la batería

- Tirar la batería puede causar un daño físico que puede afectar el funcionamiento de la batería.

Codigo de digito

Cuando se enrola un usuario en el lector de huellas, el código estándar es de 5 dígitos(su rango es de 1-65535), si necesita que el código de enrolado sea mas grande que el actual, podemos proveer un diseño personalizado para que el equipo soporte 9 dígitos de código.

Sincronización automática de tiempo

La sincronización automática de tiempo provee una solución a los problemas de mantenimiento de tiempo del sistema. Si hay muchos equipos en una red corporativa, los administradores pueden checar el tiempo manualmente en los relojes internos del sistema, pero esto es una difícil tarea, especialmente cuando múltiples sistemas están involucrados hay mucho margen de error. Este poderoso sistema de sincronización de tiempo permite que los usuarios configuren un ambiente sincronizado de tiempo a prueba de errores para las redes, sincronización automática de tiempo permite la creación de una fuente exacta de tiempo personalizada en una red corporativa estableciendo la sincronización de tiempo para cada

dispositivo en la red.

Nuestro lector de huellas se puede establecer como tiempo de Cliente y Servidor, establezca un equipo como el servidor de la red, es necesario establecer la opción de sincronizado de tiempo automático en el equipo que desea se configure la hora de acuerdo a la dirección IP del servidor, modifique la IP del cliente de tiempo para conectarse con el servidor.

Ejemplo: Hay muchos equipos que están provistos con la función de sincronización automática de tiempo, asignamos el equipo "A" como servidor de tiempo, su tiempo se muestra como YY/MM/DD, HH:MM y su dirección IP es 192.168.1.100. Hay un equipo "M" que necesita sincronizar el tiempo al mismo que tiene el equipo "A", entre al menú del equipo menú->opciones->opciones de sistema->opciones avanzadas, seleccione la opción sincronizar tiempo automáticamente, establezca la dirección IP del servidor, después de terminar asegúrese de reiniciar el equipo para que la configuración tenga efecto, después de un intervalo de tiempo el equipo buscara por el Servidor de Tiempo para sincronizarse, para mas detalles contáctenos o consiga asistencia técnica.

Horario de verano

Algunos equipos cuentan con un tiempo correcto y actual en cualquier zona horaria del mundo. Los ajustes para "Daylight Saving Time" (Horario de verano") son de acuerdo a las reglas y

leyes de cada lugar. No importa en cual periodo de tiempo se encuentra una ciudad o un país, esta es su mejor opción para un reloj.
Esta opción se puede establecer en las opciones del lector de huellas, presione la tecla MENU, entre a opciones->fecha/hora. Dependiendo el mes y la hora en la que se encuentre se puede adelantar o atrasar una hora el reloj para cambiar al horario de verano.

Establecer el horario de verano：

1、Entre a Menú->Opciones->Opciones de sistema, la opción de horario de verano (daylight saving) aparecerá, entre a esta opción para establecer el horario de verano. Se muestra lo siguiente:

Daylight Saving time	
►Daylight	Y
Daylight Saving Time	
Standard Time	

Seleccione "Daylight Saving Time" como "Yes", después de terminar de configurarlo presione "OK" para guardar los cambios, entonces el horario de verano empezará.

2、Seleccione "Daylight Saving Time" para establecer el tiempo:

MM-DD 24H
4 - 1 08：00

ESC OK

Después de establecer esta opción asegúrese de reiniciar el equipo para que los cambios tengan efecto. De acuerdo a la figura de arriba, cuando se lleguen las 8:00 en punto del primero de abril, el equipo entrara en el horario de verano, el reloj se adelantara una hora.

2、 Seleccione “Tiempo normal (Standard Time)”, introduzca la hora

Después de terminar la configuración estos cambios no tendrán efecto hasta que se reinicie el equipo, de acuerdo a la siguiente figura, cuando se lleguen las 8:00 en punto del primero de octubre, el equipo regresara a la hora normal y se atrasara una hora.

MM-DD 24H
10 - 1 08：00

ESC OK

Asignar hora para reproducir voz (por periodo de tiempo, grupo)

Junto con el sonido el usuario entra en operación en el equipo lector de huellas, por ejemplo si la autenticación es positiva el equipo dirá “Gracias!”, si la autenticación es negativa el equipo dirá “Intente de nuevo por favor”. Con el fin de obtener mas y satisfacer los requerimientos de la naturaleza humana y activar la reproducción de voz, proveemos una opción para asignar la reproducción de voz a cierto tiempo que se diseño para anunciar alguna operación de acuerdo a las diferentes necesidades y enviar una reproducción de voz de acuerdo a ellas, ejemplo: el personal entra a trabajar a las 8 en punto. Cuando una persona cheque entre las 6:00-8:00, el equipo dirá “Gracias”, si alguien llega tarde durante 8:00—10:00, el equipo dirá “llego tarde, gracias”.

Podemos realizar dos tipos de configuración.

Por periodo de tiempo: De acuerdo a un periodo de tiempo asignar un sonido diferente, para cuando un equipo entre en operación durante un periodo de tiempo asignara un sonido, durante otro periodo de tiempo el equipo emitirá otro sonido.

Por grupo: Divida a los usuarios en diferentes grupos, un grupo de usuarios utilice un sonido en particular.

Para mas detalles vea el siguiente ejemplo:

1、 Hay 8 periodos de tiempo que se pueden establecer, entre a menú→Opciones→Opciones de sistema→Opciones avanzadas, seleccione "Periodo de tiempo de voz (Time Period Voice)" para establecerlo por día, por ejemplo de 07：000-9：00 reproduce 001; de 10：00-12：00 reproduce 002:

Time Period Voice	
001	07：00 - 09：00
002	10：00 - 12：00
003	00：00 - 00：00
004	00：00 - 00：00
005	00：00 - 00：00
006	00：00 - 00：00
007	00：00 - 00：00
008	00：00 - 00：00

2、 Después de terminar la configuración, asegúrese de reiniciar el equipo para que los cambios tengan efecto.

Nota：Si desea mas detalles, por favor contacte con nuestra asistencia técnica.

Código de trabajo

Ofrecemos el concepto de "código de trabajo (Work Code)" que

dependiendo el resultado de la verificación en el equipo se distinguen diferentes eventos y proveer comodidad para trabajar con el programa de registro, hay una opción en el equipo que soporta esta función, presione Menú→Opciones→Opciones avanzadas →Work code, establezca el código de trabajo, hay tres opciones: Modo1, Modo2, Ninguno (None).

Seleccione Modo1, es decir, después de pasar la verificación de huella, asegúrese de introducir el código de trabajo, el registro de esta verificación y el código de trabajo se almacenarán juntos.

Seleccione Modo2, primeramente ingrese el código de trabajo (1-9 dígitos), después coloque el dedo para verificarse, el registro de esta verificación y el código de trabajo se almacenaran juntos.

Seleccione “Ninguno (None)”, esta función se desactivará.

Ahora el software de T&A puede almacenar este campo en las bases de datos mientras se descargan los registros, por lo tanto puede dejar de tratar con eso de acuerdo a las diferentes categorías.

Ahora la comunicación independiente SDK brinda un Segundo apoyo para desarrollar el “código de trabajo”, el usuario puede avanzar para el desarrollo. De acuerdo con las diferentes categorías que se trabaja realizara estadísticas de diferentes tipos de trabajo y maneras de verificación.

DHCP

Dynamic Host Configuration Protocol (DHCP) en un protocolo estandarizado que permite a los clientes ser dinámicamente asignados con varios parámetros de configuración, como una dirección IP, mascara de subred, default Gateway y otra información de configuración critica de red. Los servidores DHCP centralizan la administración de esos datos de configuración y son configurados por administradores de red con configuraciones que son apropiadas para un determinado ambiente de red. Los servidores DHCP se comunican con sus clientes a través del uso de “mensajes DHCP”.

Debe haber un servidor DHCP en la red cuando la función de DHCP sea activada en nuestro equipo lector de huellas, cuando el equipo está conectado en la red como un cliente DHCP, emitirá un mensaje de broadcast para la red local, después de que el servidor DHCP reciba la solicitud asignara una dirección IP dinámica y un DNS de acuerdo al estado actual en la red.

Para equipos que tienen esta función integrada entre en Menú->Opciones→Opciones de comunicación→DHCP y establezca esta opción como “Y”, el equipo lector de huellas enviara una solicitud al servidor DHCP para pedir una dirección IP cuando se conecte a la red, si esta opción se establece como “N”, el equipo no enviara esta solicitud.

Acerca de la declaración de privacidad

Estimado cliente:

Primeramente, gracias por utilizar los lectores de identificación de huella que diseñamos y producimos, como uno de los proveedores mundiales de tecnología de identificación de huella nos lleva sin cesar a la investigación y al desarrollo, también creemos que dicha acción es necesaria para: (a) cumplir con la ley o el proceso legal de nuestra empresa; (b) proteger y defender los derechos o propiedad de nuestra empresa (incluyendo la ejecución de nuestros acuerdos); o (c) regirse por las leyes de cada país o cuestiones legales que envuelven los derechos humanos y declaración de privacidad. Estamos comprometidos a proteger su privacidad.

Nos señala lo siguiente:

1. Nuestros equipos de identificación de huella se limitan a capturar puntos característicos de la huella, pero no la imagen de la huella, no involucra la privacidad.
2. Las características de la huella no sirven para recuperar la imagen original de la huella, no involucra la privacidad.
3. Somos un proveedor de material, en ningún caso somos responsables de algún daño directo o indirecto derivado del mal uso o de la incapacidad de utilizar nuestro equipo.

4. Si tiene alguna opinión diferente o alguna inconformidad con la declaración de privacidad de utilizar nuestro equipo, por favor contacte directamente con su empleador.

Nuestro equipo lector de huellas o el kit de programación provistos con la función de capturar la imagen original de la huella de las personas, si infringe alguno de sus derechos, por favor contacte con el gobierno local o el proveedor final del equipo, como el productor inicial del equipo no tenemos ninguna responsabilidad legal por el daño que pueda causar.

Nota: Hay derechos limitados a la privacidad y derechos humanos en la constitución de China.
La dignidad personal de los ciudadanos de la República popular de China es inviolable y, además, los insultos, difamación, falsa acusación o incriminación directa contra sus ciudadanos por cualquier medio están prohibidos por la protección de la libertad de las personas y residentes. La Constitución provee la libertad y la privacidad que corresponde a los ciudadanos.

Por último hacemos hincapié que como una clase de tecnología avanzada de identificación de huellas, la identificación de huella aplicara en el futuro a comercio electrónico, bancos, seguros, industria de servicio de leyes; cada año en todo el mundo es afectado por la falta de seguridad en las contraseñas, la humanidad está sufriendo grandes pérdidas. En virtud de la seguridad y los ambientes seguros la identificación por huella protege su estado de posibles daños.